Grundwissen Netzwerke und Internet

Lernheft 10

Drahtlose Technologien

Inhaltsverzeichnis:

10.1	Einleitung	3
10.2	Grundlagen WLAN	4
10.2.1	Einleitung	4
10.2.2	Standard und Definition	7
10.2.3	802.11n – Die neue Technik	8
10.3	Medienzugriff im WLAN	13
10.3.1	CSMA/CA	13
10.3.2	Versteckte und ausgelieferte Stationen	14
10.3.3	Wartezeiten	15
10.4	WLAN-Betriebsarten	17
10.4.1	Infrastruktur-Modus	18
10.4.2	Adhoc-Modus	20
10.4.3	Wireless Distribution System	23
10.5	WLAN-Geräte	24
10.5.1	Client-Hardware	25
10.5.2	Access-Point	28
10.5.3	Kombi-Geräte	31
10.6	WLAN-Hotspots	35
10.7	WLAN-Roaming	37
10.8	WLAN Schwachstellen	38
10.9	Das WLAN der Zukunft	40

© Copyright Laudius GmbH

10.10	Bluetooth	42
10.10.1	Hardware/Geräte	42
10.10.2	Architekturen	44
10.10.3	Die Standards	46
10.10.4	Die Technik	47
10.10.5	Die Frequenzen vom Bluetooth	48
10.10.6	Sicherheit	49
10.10.7	Anwendung	51
10.11	Die Funkstandards im Vergleich	53
10.12	WiMax	55
10.13	Selbstlernaufgaben	58
10.14	Zusammenfassung und Ausblick	59
10.15	Hausaufgabe	61
10.16	Lösungen zu den Selbstlernaufgaben	62

10.1 Einleitung

In den letzten Jahren hat die Nutzung drahtloser Netzwerke zur Verbindung von Computern im Nahbereich, sogenannter WLANs (Wireless Local Area Network), stark zugenommen.

Gegenüber einem drahtgebundenen Netzwerk, etwa auf Basis von

– Twisted-Pair Kabel oder

– Glasfaserkabel

bietet ein Funknetzwerk den Vorteil, dass keinerlei Übertragungskabel angeschlossen und verlegt werden müssen.

Computer können per Funkübertragung innerhalb einer bestimmten Reichweite untereinander Daten austauschen, sofern Sie

– über die notwendige Hardware (z. B. WLAN-Adapter oder Bluetooth-Modul) verfügen und

– entsprechend konfiguriert sind.

Mit dem jüngsten Standard 802.11n sind die Übertragungsgeschwindigkeiten von WLAN-Technologie der Bandbreite von Kabelnetzwerken erheblich näher gekommen; mittlerweile gibt es sogar Funkstrecken, auf denen die Datenrate die Geschwindigkeit manches kabelgebundenen LANs übersteigt. Der Rückstand zu Ethernet hat sich in den vergangenen Jahren deutlich verringert.

Wireless LAN ist ein lokales Netzwerk, das auf Funkbasis arbeitet. Hier werden die Endgeräte des Netzwerkes mit Funkzubehör ausgerüstet und die Datenübertragung läuft kabellos. Allerdings ist WLAN nicht die einzige Funktechnologie.

Bei der Vernetzung von Kleingeräten im Haushalt und Geräten der Kommunikations-elektronik kommt häufig Bluetooth zum Einsatz. Auch die Entwicklung von Bluetooth schreitet in großen Schritten voran.

Inhalt dieser Lerneinheit sind die drahtlosen Netzwerktechnologien.

Ziel dieses Lernheftes ist es, dass Sie Funkübertragung als die zukunftsweisende Technik bei fast jedem Vernetzungsszenario kennen lernen. Speziell in Heim- und Unternehmensnetzwerken spielt Funk schon heute eine entscheidende Rolle.

Sie werden die verschiedenen Funktechnologien kennen lernen, die Sie für die kabellose Datenübertragung in Netzwerken einsetzen können. Die Begriffe

– WLAN,

– IrDA,

– Bluetooth und

– WiMax

werden für Sie keine Fremdwörter mehr sein.

Wie auch beim Ethernet verwenden wir im Funknetzwerk

– Netzwerkadapter,
– Konfigurationsprogramme,
– Verteiler,
– Router,
– Steuergeräte,
– Zugriffsverfahren,
– Diagnose-Tools,

welche sämtlich internationale Standards unterstützen.

Allerdings macht, wie Sie wissen, auch die Entwicklung der Ethernet-Standards nicht halt; 10 Gigabit pro Sekunde stellen eine extrem hohe Messlatte dar, welche die heutigen bezahlbaren Funktechniken (für den Heimbereich und kleine Netzwerke) bei Weitem noch nicht erreichen.

Diese Lerneinheit vermittelt Ihnen

– technische Eigenschaften der drahtlosen Netzwerke,
– WLAN-Grundlagen,
– Kenntnisse über Bluetooth,
– welche Rolle WiMax bei der Funkübertragung spielt,
– einen Vergleich der Funktechnologien.

Lernziele:

Sie können nach Durcharbeitung dieses Lernhefts
– die grundlegenden technischen Eigenschaften der Funkübertragung kennen.
– die Funktechniken nach Zielsetzung und Anwendungsbereichen unterscheiden.
– die aktuellen Funkstandards kennen.
– den Aufbau und die Architekturen von WLANs erläutern.

10.2 Grundlagen WLAN

10.2.1 Einleitung

Funktechnik wird oft eingesetzt, damit von mehreren Rechnern bzw. Anwender/-innen ein einziger Zugang zum Internet gleichzeitig genutzt werden kann. Musste bei klassischer Ethernet-Technologie stets eine Kabelverbindung von der Telefonanschlussdose oder vom Kabelmodem, über die auch breitbandige DSL-Anschlüsse geschaltet werden, zu jedem einzelnen Rechner gelegt werden, so genügt es nunmehr, dass nur ein Vermittlungsgerät - ein Router mit WLAN-Schnittstelle - unmittelbar an die Internetleitung angeschlossen wird und per Funk mit den Netzwerkteilnehmern kommuniziert.

Diejenigen Computer, die eine Internetverbindung benötigen, nehmen lediglich Funkkontakt mit dem WLAN-Router auf, der dann die eingehenden Anfragen an den Web-Server weiterleitet.

In welchen Bereichen setzen wir drahtlose Kommunikation ein? Die folgende Tabelle gibt Ihnen eine Antwort:

Anwendungen der drahtlosen Kommunikation			
Bereich	**Technik**		**Anwendung/Dienst**
Telefonie	GSM	Global System for mobile Communications	D1- und D2-Netz
	DECT	Digital European Cordless Telecommunications[1]	Schnurloses Telefon
Rufsysteme			Paging-Geräte (Quix, Scall)[2]
Privatfunk	TETRA	Terrestrial Trunked Radio[3]	Bündelfunk auf Baustellen, zwischen Busfahrern
Geräteverbindung		Bluetooth	Piconetze für Kleinstgeräte in Wohnung, Büro
Punkt zu Punkt Verbindungen	IrDA	Infrared Data Association[4]	Druckerschnittstelle
Satelliten	GPS	Global Positioning System[5]	Positionierungssysteme

Tab. 1: *Funktechnik in der Praxis*

Größere Funknetzwerke bestehen aus vielen einzelnen Funkzellen. Dabei bildet in jeder Zelle ein WLAN-Router die zentrale Netzkomponente; er steuert den Datentransfer zwischen den Endgeräten und verbindet seine eigene Zelle mit anderen Funkzellen oder leitungsgebundenen Netzwerken.

1 Zum DECT-Standard siehe http://artikel.4.am/archives/2566-Was-ist-ein-DECT-Telefon.html

2 Paging (Funkruf) ist ein Verfahren, Nachrichten über ein Funknetz an kleine Empfangsgeräte zu senden, siehe dazu http://www.teltarif.de/i/paging.html

3 Siehe etwa http://www.pressebox.de/attachment/146694/tetra-info.pdf

4 Zur Infrarotübertragung siehe etwa http://de.wikipedia.org/wiki/Infrared_Data_Association

5 Informationen zu GPS finden Sie z. B. unter http://www.ipe.uni-bonn.de/vorlesung/xPFa/XPfa_GPS.DOC

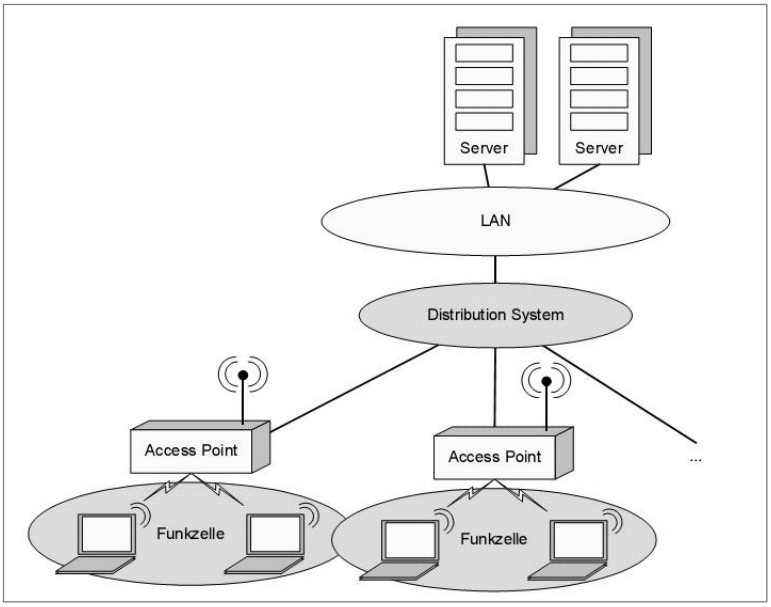


Abb. 1*: WLAN-Zellen*

Die Abbildung zeigt zwei Funkzellen, welche jeweils von einem Funk-Router (Basisstation, Access-Point) verwaltet werden. Über ein Verteilersystem (Wireless Distribution System, WDS) sind sie untereinander und mit einem lokalen Kabelnetzwerk verbunden.

Das Distribution System besitzt unter anderem die Funktion einer Bridge, so dass auch weitere Netzwerke an das System angeschlossen werden können.

Je nach Position der einzelnen Rechner und Größe des Netzwerkes tritt beim Senden im Funknetzwerk eine neue Situation auf: Nicht jede Station kann jede andere hören bzw. wahrnehmen.

Der Zugriff auf das Medium könnte im Funknetzwerk auf gleiche Weise wie im Ethernet erfolgen. Das funktioniert allerdings nur, solange sämtliche Stationen miteinander in Funkkontakt stehen. Ansonsten würde eine der Stationen das Medium als frei erkennen, obwohl eine andere Station sendet, das Medium also belegt.

Ein mögliches Szenario zeigt die folgende Abbildung:

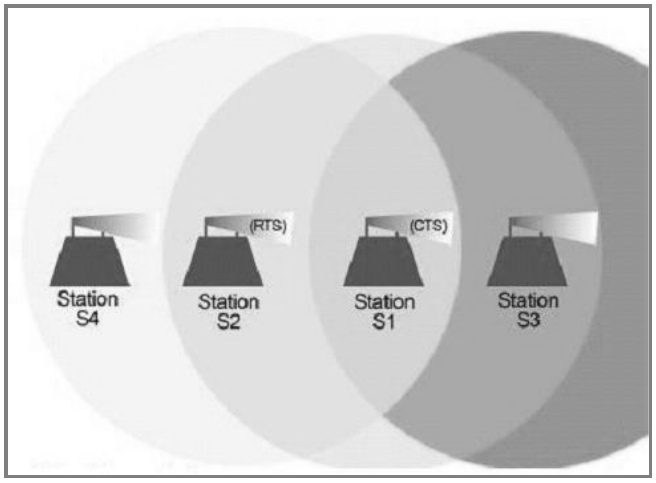


Abb. 2: *Versteckte Stationen im WLAN*

Station S1 kann hier von den zwei Stationen S2 und S3 Daten empfangen. Ein unmittelbarer Funkkontakt zwischen S2 und S3 ist dagegen nicht möglich.

Sendet nun S2 eine Nachricht an S1, so erscheint das Medium dennoch für S3 als frei und es kann zu einer Kollision kommen, d. h. es entsteht ein Datencrash, wenn S3 ein Datenpaket an S1 sendet.

Auch S4 und S3 erkennen sich nicht gegenseitig. Würde also S4 zur gleichen Zeit wie S3 ein Datenpaket an S2 senden, so könnte S2 es nicht fehlerfrei empfangen.

Sie erkennen: Nach der Logik von CSMA/CD kann die Sendestation in vielen Fällen keine Kollision erkennen. Anders als bei drahtgebundenen Medien lässt sich bei Funknetzen nur auf Empfängerseite prüfen, ob eine Kollision vorliegt.

Um solche Situationen zu vermeiden, beinhaltet die 802.11-Norm den RTS-CTS Mechanismus. Ein Request-To-Send Rahmen (RTS) wird von der sendewilligen Station an den Empfänger übertragen und von diesem mit einem Clear-To-Send Rahmen (CTS) beantwortet. Klappt dieser Austausch problemlos, so beginnt der Sender nach einer kurzen Wartezeit die Datenübertragung.

10.2.2 Standard und Definition

Ein Wireless-LAN, WLAN oder Wi-LAN ist ein lokales Netzwerk mit Funkübertragung. Wie auch für Ethernet hat das Institute of Electrical and Electronic Engineers (IEEE) für funkbasierte Netze zahlreiche Normen bzw. Standards erarbeitet; diese sind in der Familie der IEEE 802.11-Standards zusammengefasst.

Der erste Standard der IEEE 802.11-Familie wurde 1997 freigegeben. Bis dahin war an den breiten Einsatz drahtloser Datennetze wegen fehlender Standards und der geringen Datenübertragungsrate nicht zu denken.

IEEE 802.11 ist das Analogon zur IEEE 802.3-Norm; die 802.11-Norm des IEEE enthält die verbindlichen Standards für kabellose Datenübertragung, indem sie die Bitübertragungsschicht des OSI-Schichtenmodells für ein WLAN definiert.

Unabhängig von den verwendeten Netzwerkprotokollen lässt sich WLAN-Hardware in jedes Netzwerk einbinden. Daher ist es ohne Einschränkung möglich, eine (kabelbasierte) Ethernet-Verbindung (IEEE 802.3-Standard) gegen eine WLAN-Verbindung (nach IEEE 802.11) zu ersetzen.

Der Begriff "Wireless LAN" darf dabei nicht mit der Norm "IEEE 802.11" verwechselt bzw. gleichgesetzt werden: Während „Wireless LAN" einfach die allgemeine Bezeichnung für ein kabelloses lokales Netzwerk darstellt, ist IEEE 802.11 ein Regelwerk, das vorschreibt, wie ein WLAN aufzubauen ist. Hier wird die software- und hardwaretechnische Implementierung festgelegt. Es könnte also durchaus auch andere Standards geben, die den Aufbau von Wireless LANs festlegen.

Die allererste IEEE 802.11-Norm beschreibt den ursprünglichen Standard, der Übertragungsraten von bis zu 2 MBit/s möglich macht. Um die Übertragungsrate und die Datensicherheit zu verbessern, wurde der Standard mehrfach erweitert:

Standard	802.11	802.11b	802.11b+	802.11a/h/j	802.11g	802.11n
Frequenz-bereich	2,4 GHz	2,4 GHz	2,4 GHz	5 GHz	2,4 GHz	2,4 GHZ, 5 GHz
Datendurchsatz maximal	2 MBit/s	11 MBit/s	22 MBit/s	54 MBit/s	54 MBit/s	300 MBit/s
Kompatibel zu	802.11b	802.11b+/g	802.11b/g	-	802.11b/b+	802.11b/g

Tab. 2: *Ausgewählte WLAN-Standards*

Die Bezeichnung „IEEE 802.11“ steht einerseits für die allererste Version der WLAN-Standards von 1997, andererseits für die Gesamtheit/Familie aller IEEE 802.11-Normen, die bis heute veröffentlicht wurden. Um Irritationen auszuschließen, bezeichnet „IEEE 802.11“ im Rahmen dieses Lehrgangs – soweit es nicht explizit anders vermerkt ist – die Norm/Familie als Ganzes und nicht die einzelne ursprüngliche Version.

Im Zusammenhang mit IEEE 802.11 und Wireless LAN fällt sehr häufig der Begriff WiFi, der für Wireless Fidelity[6] steht und von der Wireless Ethernet Compatibility Alliance (WECA)[7] kommuniziert wird. Die WECA ist ein Zusammenschluss von Firmen, die mit dem WiFi-Logo ihre Produkte als IEEE 802.11-kompatibel kennzeichnen.

Diese Geräte haben eine Art TÜV durchlaufen. Produkte mit diesem Logo lassen sich uneingeschränkt mit Produkten anderer Hersteller kombinieren. Das bedeutet, dass im selben Netzwerk eingesetzte Wireless-Hardware, nämlich

– WLAN Access-Point und

– WLAN-Client

von unterschiedlichen Herstellern stammen können.

Somit können die Bezeichnungen „WiFi“ und „WLAN“ als gleichbedeutend angesehen werden.

Kommen wir nun nach einigen allgemeinen Betrachtungen zum derzeitigen WLAN-Standard, nämlich zu der Norm 802.11n.

10.2.3 802.11n – Die neue Technik

Die Norm IEEE 802.11n beschreibt den heutigen WLAN-Standard. Sie ist die Spezifikation für ein WLAN mit Übertragungsraten von 150, 300, 450 und 600 MBit/s. Für die Entwicklung der IEEE 802.11n wurde Ende 2003 eine Arbeitsgruppe eingerichtet, um einen WLAN-Standard zu schaffen, der eine Nettoübertragungsrate von mindestens 100 MBit/s erreicht.

6 Zur Definition von WiFi siehe http://www.drweb.de/magazin/was-ist-lexikon-wifi/

7 Die WECA heißt heute WiFi Allianz, siehe dazu http://www.elektronik-kompendium.de/sites/net/0610051.htm
Sie nimmt die Zertifizierung der WLAN-Geräte vor.

Wie bei Fast-Ethernet sollten im WLAN auch 100 MBit/s möglich sein. Geschwindigkeiten von 1 Gigabit pro Sekunde oder gar 10 Gigabit pro Sekunde, wie sie beim Ethernet möglich sind, sind allerdings noch in weiter Ferne.

In der Praxis ist mit 120 MBit/s (bei 300 MBit/s brutto) und 240 MBit/s (bei 600 MBit/s brutto) zu rechnen.

Erreicht werden diese Geschwindigkeiten durch

– mehrere Antennen und Signalverarbeitungseinheiten (MIMO),
– die Verdopplung der Funkkanal-Bandbreite auf 40 MHz, sowie
– die parallele Nutzung des 2,4 GHz- und 5 GHz-Frequenzbandes.

Der Standard IEEE 802.11n wurde im September 2009 verabschiedet. Er beinhaltet zahlreiche Techniken zur grundlegenden Verbesserung der Übertragungsrate:

– Antennengruppen mit MIMO (Multiple Input Multiple Output),
– spatial Multiplexing mit Space Time Block Coding (STBC)[8],
– Antennen-Diversity (bei mehreren Antennen wird das Signal von derjenigen Antenne mit dem besseren Empfang abgegriffen),
– verbesserte OFDM-Modulation mit maximal 65 MBit/s in einem 20 MHz-Kanal (nur 54 MBit/s bei IEEE 802.11g)[9],
– Kanalbündelung,
– Transmit Beamforming,
– Packet Aggregation (Zusammenfassen von Paketen),
– RIFS (Reduced InterFrame Spacing),
– Greenfield-Mode
(Abschaltung der 802.11a-, 802.11b- und 802.11g-Unterstützung).

Bei IEEE 802.11n wird der Datendurchsatz über 100 MBit/s durch einen höheren Durchsatz auf der MAC-Schicht (Media Access Control, Bitübertragungsschicht im OSI-Modell) und einen geringeren Overhead erreicht. Ein deutlicher Geschwindigkeitszuwachs wird dadurch erreicht, dass die Bandbreite unter allen Teilnehmern besser aufgeteilt wird.

---

8 STBC (die Raum-Zeit Block Codierung) ist ein Übertragungsverfahren in Funknetzwerken, bei dem die zeitliche, die spektrale und auch die räumliche Dimension der Übertragungsstrecke ausgenutzt wird.

9 OFDM (Orthogonal Frequency Division Multiplexing) ist ein digitales Modulationsverfahren, das in verschiedenen Kommunikationssystemen zum Einsatz kommt. Wesentlich bei OFDM ist eine hohe spektrale Effizienz. Das heißt, es lassen sich mehr Daten pro Bandbreite übertragen als bei herkömmlichen Modulationsverfahren. OFDM toleriert auch Umgebungen mit hoher HF-Überlagerung. Einige Dienste, die OFDM einsetzen wie z.B. WLAN, arbeiten in den nicht regulierten ISM-Bändern (Industrial, Scientific, Medical), in denen auch viele andere nicht regulierte Geräte arbeiten, wie analoge schnurlose Telefone (900 MHz), Mikrowellenherde (2,45 GHz), Bluetooth-Geräte (2,45 GHz), digitale schnurlose Telefone (2,45 GHz oder 5,8 GHz) und WLAN (2,45 GHz oder 5,8 GHz). Außerdem funktioniert OFDM problemlos in Umgebungen mit starker Mehrwegausbreitung. Siehe dazu etwa http://www.elektroniknet.de/home/mobilfunk-spezial/fachwissen/ofdm-die-modulation-der-zukunft/

Im Vergleich zu älteren 802.11-Standards verbessern

– Transmit Beamforming (Sendestrahlsteuerung)[10],
– Receive Combining[11] und
– breite Hochfrequenzkanäle

die Funkverbindung und bringen mehr Datendurchsatz. Je nach Anwendung oder lokaler Frequenzvergabe (abhängig von der Regulierung) sind 10, 20 oder 40 MHz breite HF-Kanäle möglich.[12].

Die WLAN-Geräte prüfen, ob diese Kanäle für die Datenübertragung frei sind. Bluetooth-Geräte in der Nähe können den WLAN-Geräten mitteilen, nur einen Kanal zu nutzen. So bleibt auch für gleichzeitige Bluetooth-Funkverbindungen noch genug Bandbreite übrig.

Da die Funkschnittstelle einer ständigen Veränderung unterliegt, werden vor der Nutzdatenübertragung Trainingssequenzen übertragen. Mit Hilfe von Pilottönen innerhalb der Nutzdaten erfolgt dann eine dynamische Feinabstimmung der Signalverarbeitung. Bei Einsatz in Räumen nutzt die neue Technik die Reflektionen (mehrfache Empfangssignale) für mehr Datendurchsatz aus.

Nach IEEE 802.11n kann sowohl im 2,4 GHz- als auch im 5 GHz-Band übertragen werden. Das bedeutet, es stehen zwei Frequenzbänder zur Verfügung, allerdings senden die meisten weniger teueren 802.11n-Geräte nur auf dem 2,4 GHz-Band.

Kanalnummer	mittl. Frequenz [MHz]	Bereich [MHz]
1	2412	2401-2423
2	2417	2406-2428
3	2422	2411-2433
4	2427	2416-2438
5	2432	2421-2443
6	2437	2426-2448

[10] Die Implementierung der Transmit-Beamforming-Technologie (TxBF) ermöglicht die präzise Fokussierung des zu sendenden Signals auf den Ort des WLAN-Clients. Die optimale Einstellung der Sendeparameter ermöglicht hat die maximale Stärke des Sendesignals beim Empfänger zur Folge. So kann der Datendurchsatz (nach Herstellerangaben) um etwa 50 % erhöht werden. Siehe dazu www.fritz.de.

[11] Receive Combining (oft auch als Antenna Diversity oder Antennendiversität bezeichnet) ist ein Verfahren, bei dem mehrere Antennen pro Sender oder Empfänger verwendet werden, um Überlagerungen bzw. Interferenzen bei der Funkübertragung zu reduzieren. Bei der Ausbreitung von Funkwellen können Reflexionen an Hindernissen oder dem Erdboden auftreten. So löschen sich oft zwei Signale ganz oder teilweise gegenseitig aus, denn es kommt zwischen beiden zu einem Gangunterschied bzw. zu einer Phasenverschiebung und damit zu einer Signalschwächung. Besitzt der Empfänger mehrere Antennen, so es wahrscheinlich, dass mindestens eine der Antennen nicht von der Signalauslöschung betroffen ist. Bei Receive Combining ist im Empfängergerät eine Logik implementiert, die erkennt, welche der Antennen gerade das beste Signal empfängt, und dann deren Signal verwendet.

[12] Ein Hochfrequenz-Kanal (High Frequency, HF) im WLAN ist derjenige für alle Geräte gleichermaßen festgelegte Frequenzbereich im 2,4 oder 5 GHz-Band, auf dem die Übertragung innerhalb desselben Netzwerkes zwischen den Clients bzw. zwischen Router und Clients stattfindet.

Kanalnummer	mittl. Frequenz [MHz]	Bereich [MHz]
7	2442	2431-2453
8	2447	2436-2458
9	2452	2441-2463
10	2457	2446-2468
11	2462	2451-2473
12	2467	2456-2478 (nur EU)
13	2472	2461-2483 (nur EU)

Tab. 3: *WLAN-Kanalzuordnung im 2,4 GHz-Band*

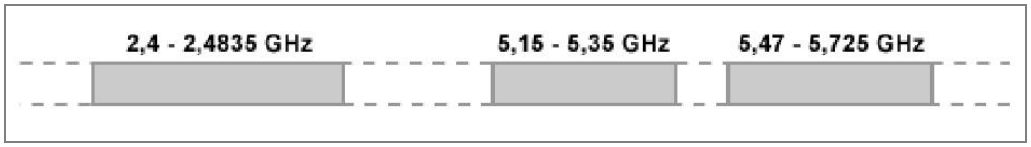


Abb. 3: *WLAN-Frequenzen*

Eine Übersicht über die WLAN-Kanäle im 5 GHz-Bereich finden Sie unter http://de.wikipedia.org/wiki/IEEE_802.11.

Die Technik **Packet Aggregation**, gelegentlich auch als **Concatenation** bezeichnet, war in den älteren WLAN-Standards 802.11b/a/g nicht definiert; sie nutzt den Umstand, dass ein WLAN-Frame bis zu 2304 Byte enthalten darf, aber in der Praxis oft deutlich kleinere Nutzdatenpakete vorkommen.

Packet Aggregation fügt mehrere kleine Pakete zu einem WLAN-Frame zusammen, was Medienzugriffe und Empfangsbestätigungen bzw. Quittierungen (Acknowledges) spart. Manche Hersteller vergrößerten gar den WLAN-Frame, sodass er entgegen der damaligen Norm bis zu zwei Ethernet-Pakete voller Größe (2×1518 Byte) enthielt. Bei 802.11n gehört Packet Aggregation endlich zum Standard, ein WLAN-Frame darf nun bis zu 7955 Byte enthalten.[13]

Die Technik Multiple Input Mulitple Output (MIMO) sieht vor, mehrere Sende- und Empfangsantennen zu verwenden. Vom Prinzip her wird der Frequenz-Zeit Matrix eine dritte Dimension, der Raum, hinzugefügt. Mehrere Antennen vermitteln dem Empfänger räumliche Informationen, was zur Steigerung der Übertragungsrate durch Spatial Multiplexing genutzt werden kann. Dabei werden mehrere Datenströme parallel auf einem Funkkanal übertragen.

Die parallele Signalverarbeitung bringt verbesserten Signalempfang und vermindert die Nachteile durch Mehrwegeempfang, der durch reflektierte Signale entsteht. Insgesamt verbessert sich die Leistung des ganzen Funksystems durch MIMO erheblich.[14]

Spatial Multiplexing bezeichnet die parallele Übertragung mehrerer Datenströme auf einem Funkkanal. Voraussetzung dafür ist der Einsatz mehrerer Antennen (MIMO). Pro Datenstrom ist eine Antenne notwendig. Der Einsatz mehrerer Antennen setzt

[13] Siehe dazu etwa http://www.heise.de/netze/artikel/Detailverbesserungen-223738.html

[14] Weitere Informationen zu Mimo finden Sie unter http://www.elektronik-kompendium.de/sites/net/1004251.htm

einen Mindestabstand zwischen den Antennen voraus; nur dann kann Spatial Multiplexing funktionieren.
Bei kleinen Geräten allerdings ist dieser Abstand nicht immer realisierbar.

Mit IEEE 802.11n ist es möglich, mehrere 10, 20 oder 40 MHz breite Kanäle innerhalb des freigegebenen Frequenzbandes bei 2,4 und 5 GHz zu nutzen. Pro 40 MHz-Kanal sind rein rechnerisch 150 MBit/s möglich. Mit zwei parallel betriebenen Datenströmen (Spatial Multiplexing) erreicht man theoretisch 300 MBit/s.

Die Hersteller geben als technische Eigenschaft ihrer Produkte immer die theoretische Datenübertragungsrate an; viel realistischer sind allerdings bei den meisten Geräten nur 40% davon, oder sogar weniger.

In der Praxis wird – so wie es auch bei allen anderen Übertragungstechniken im Netzwerk der Fall ist – die theoretische (Brutto-)Übertragungsrate bei Weitem nicht erreicht. Je nach

– Qualität/Sendestärke der Antennen,
– Signaldämpfung durch Störsender,
– auftretender Reflexion oder Beugung,
– Hindernissen zwischen Sender und Empfänger

erreicht man tatsächlich eine erheblich geringere Datenübertragungsrate.

Zusätzlicher Performanceverlust entsteht durch den Overhead, der etwa

– Verwaltungsdaten,
– Quittierungspakete (Acknowledges),
– Verschlüsselungsinformationen

umfasst, sowie durch etwaige Kollisionen.

Um eine Übertragungsrate von 600 MBit/s (brutto) zu erreichen, müssen vier räumlich getrennte Datenströme auf dem selben Kanal parallel übertragen werden. Pro Datenstrom ist eine separate Antenne erforderlich - ein hoher Hardware-Aufwand: 4 Antennen mit eigenen Sende- und Empfangseinheiten sind eine teure Konstruktion.

Anzahl der Datenströme	Übertragungsrate	
	Brutto	Netto
1	150 MBit/s	ca. 60 MBit/s
2	300 MBit/s	ca. 120 MBit/s
3	450 MBit/s	ca. 180 MBit/s
4	600 MBit/s	ca. 240 MBit/s

Tab. 4: *Maximal erreichbare Datenraten nach IEEE 802.11n*

Im Kabelnetzwerk fließen die Daten nach wie vor schneller und die Infrastruktur ist im Regelfall kostengünstiger einzurichten. Die Aufholjagd von WLAN geht daher weiter; in den kommenden Jahren werden deutliche Fortschritte erwartet – und neue Standards.

Wie im Ethernet durch CSMA/CD ist auch im WLAN der Zugriff auf das Übertragungsmedium – die Funkkanäle – klar geregelt. Einzelheiten dazu erfahren Sie im folgenden Abschnitt.

10.3 Medienzugriff im WLAN

10.3.1 CSMA/CA

Um Datenkollisionen zu vermeiden, findet im WLAN beim Zugriff auf das Medium (Bitübertragung, Schicht 1 des OSI-Modells) die CSMA/CA-Technik (Carrier Sense Multiple Access with Collision Avoidance) Anwendung, welche CSMA/CD (Carrier Sense Multiple Access with Collision Detection) im Ethernet entspricht.

CSMA/CA ist eine modifizierte Version des CSMA/CD-Zugriffsverfahrens, hauptsächlich für WLANs. Wie bei CSMA/CD hören alle teilnehmenden Stationen physikalisch den Verkehr auf dem Übertragungsmedium mit.

Bei CSMA/CA wird vor dem Versenden von Daten ein Warnpaket versendet, so dass andere Rechner darauf reagieren können und den Übertragungsvorgang abwarten. Diese Methode erhöht die Netzwerklast drastisch, da immer ein Warnpaket dem eigentlichen Datenpaket vorausgeht. Im WLAN können die Stationen so erkennen, was die anderen Teilnehmer im Netz tun, und ihr eigenes Verhalten dementsprechend anpassen. Daher kann das Netz besser ausgelastet werden. Protokolle, bei denen Stationen einen Träger (Carrier) abhören und entsprechend handeln, heißen **Trägererkennungsprotokolle** (Carrier Sense Protocols).[15]

Wenn zwei Stationen den Kanal als frei erkennen und gleichzeitig zu senden beginnen, werden beide fast sofort eine Kollision feststellen.

Wenn eine Station übertragen will, wartet sie, bis das Medium frei ist. Danach wartet sie noch eine vorbestimmte Zeitperiode (DIFS)[16] plus einer zufällig gewählten Zeitspanne, bevor sie ihren Frame überträgt. Auch in dieser Zeitspanne (Wettbewerbsfenster) wird das Übertragungsmedium weiter überwacht.

Wenn keine andere Station innerhalb des Wettbewerbsfensters vor dem gewählten Zeitpunkt mit der Übertragung beginnt, sendet die Station ihren Frame. Hat aber eine andere Station innerhalb der Wartezeit mit der Übertragung begonnen, wird der Zeitzähler angehalten und nach der Übertragung der anderen Station weiter verwendet.

---

[15] Siehe dazu http://www.melzkaffee.info/informatik/netzwerke_und_internet/infoblatt%20netzwerke.pdf

[16] Zwischen den Datenpaketen koordinieren unterschiedlich lange Wartezeiten den Zugriff auf das Funkmedium. Das DIFS (Distributed Coordination Function Interframe Space) kennzeichnet die Backoffzeit, in der eine Station das freie Funkmedium erkennen kann. Auf die verschiedenen Wartezeiten werden wir in einem der folgenden Abschnitte genauer eingehen.

Auf diese Weise gewinnen Stationen, die nicht übertragen durften, an Priorität und kommen mit einer erhöhten Wahrscheinlichkeit in den nächsten Wettbewerbsfenstern zum Zug.

Die Erkennung von Kollisionen ist ein analoger Prozess. Die Hardware, also der WLAN-Adapter der Station, muss während der Übertragung das Medium abhören. Unterscheidet sich dabei das Gesendete vom Gelesenen, ist klar, dass eine Kollision stattgefunden hat. Die Unterscheidung erfolgt, indem die Leistung oder die Impulsbreite des empfangenen Signals mit der des gesendeten Signals verglichen wird.

Eine Kollision kann nur entstehen, wenn zwei oder mehrere Stationen die gleiche Zeitscheibe auswählen. Diese Stationen müssen die Wettbewerbsprozedur erneut durchlaufen. In IEEE 802.11 ist CSMA/CA standardisiert.

Der Verbindungsaufbau im WLAN erfolgt per Handshake:

1. Der potentielle Sender sendet ein Request-to-send Signal (RTS).
2. Vom Empfänger wird dieses Signal mit einem Clear-to-send Signal (CTS) beantwortet.
3. Ist das Clear-to-send Signal beim Sender angekommen, dann wird gesendet, andernfalls wird abgebrochen.

10.3.2 Versteckte und ausgelieferte Stationen

Das im Ethernet eingesetzte CSMA/CD ist für Funknetze nicht geeignet, da nicht immer jede Station alle anderen hören kann; in drahtlosen Netzen kann es nämlich versteckte (nicht erreichbare) Stationen geben, die senden ohne dass es jede andere Station mitbekommt.

Drahtlose Netze unterscheiden sich in Bezug auf den gemeinsamen Medienzugriff durch wichtige Faktoren von drahtgebundenen Netzen:

– Der Netzadapter ist nicht notwendigerweise vollduplex-fähig. Während einer eigenen Übertragung kann das Medium nicht überwacht werden. Der Einsatz eines „Collision Detection“-Mechanismus, wie er etwa von CSMA/CD vorgesehen ist und bei Ethernet verwendet wird, würde dann fehlschlagen. Deswegen wurde CSMA/CD ein Mechanismus hinzugefügt, der konsequenter dem Prinzip „listen before talk“ („erst hören, dann sprechen“) folgt. An die Stelle der Kollisionserkennung („CD“) tritt die bestmögliche Kollisionsvermeidung („CA“). Dadurch lassen sich gleichzeitige Datenübertragungen zwar nicht völlig verhindern, jedoch die Wahrscheinlichkeit, mit der dieser Fall eintritt, erheblich verringern.

– Die Reichweite des Signals ist stark begrenzt, da die Stärke des Empfangspegels umgekehrt proportional zur quadratischen Entfernung zwischen Sender und Empfänger ist, also quadratisch mit der Entfernung abnimmt; in der Praxis bedeutet dieser Sachverhalt beispielsweise, dass bei doppeltem Abstand zweier Stationen die Signalstärke beim Empfänger nur noch bei 25 % Prozent liegt. Deshalb kann es zu Effekten wie „versteckten“ oder „ausgelieferten“ Endgeräten kommen.

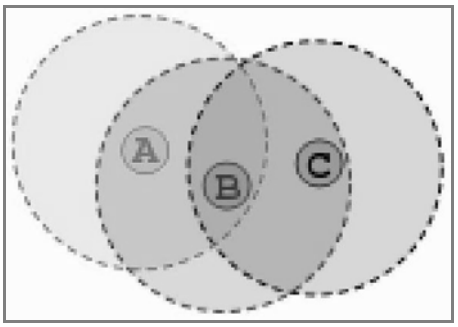


Abb. 4: *Versteckte Station: A und C erkennen sich gegenseitig nicht*

Zu einem versteckten Endgerät (hidden station bzw. hidden terminal) kommt es zum Beispiel bei dem in der Abbildung dargestellten Szenario: Die zwei Funkteilnehmer A und C sind räumlich so weit von einander entfernt, dass sie ihre Funksignale gegenseitig nicht empfangen können. Zwischen ihnen befindet sich die Station B. A und C senden nun zeitgleich an B und sorgen so für einen Datencrash, können diesen aber nicht erkennen, da sie die Funksignale des jeweils anderen nicht unmittelbar empfangen können. A ist für C ein verstecktes Endgerät und umgekehrt.

Ein ausgeliefertes Endgerät (exposed station bzw. exposed terminal) liegt vor, wenn in unserem vorliegenden Szenario die Station B an A sendet und nun C an irgendeine andere Station senden möchte, die sich nicht im Sendebereich von B befindet. C erkennt die Signale von B und wartet, bis die Übertragung zwischen B und A vorbei ist. Da die Funkwellen von C aber Station A gar nicht erreichen können, wäre es gar nicht nötig zu warten; bei A könnte gar kein Konflikt auftreten. Dennoch ist C von der Sendung der anderen beiden Stationen abhängig (ausgeliefert).

Um das Problem der versteckten Endgeräte zu vermindern, ist eine Koordination durch „Request to Send / Clear to Send“ (RTS/CTS)-Erweiterung für CSMA/CA definiert. Dabei muss die sendewillige Station den Kanal durch ein RTS-Paket reservieren. Der Empfänger bestätigt diese Reservierung mit einem CTS-Paket. Anschließend ist ein sofortiges Senden der Daten möglich. Andere Stationen speichern die Belegungsdauer, die im RTS- und CTS-Paket mitgeteilt wurde, und senden während dieser Zeit keine Daten.

Das Problem der „ausgelieferten“ Endgeräte (exposed terminal) wird vom WLAN-Standard nicht gelöst, ist aber auch nicht so dramatisch einzustufen wie das Hidden-Terminal-Problem, da es lediglich zu einem geringeren Durchsatz führt.

10.3.3 Wartezeiten

Der Zugriff auf das Medium geschieht beim WLAN über den CSMA/CA-Algorithmus, Carrier Sense Multiple Access with Collision Avoidance:

– Multiple Access deutet an, dass mehrere Kommunikationsteilnehmer wie zu alten Zeiten im Ethernet einen gemeinsamen Übertragungskanal nutzen (Shared Medium).

– Carrier Sense zeigt an, dass jeder Kommunikationsteilnehmer den gemeinsamen Kanal überwacht und seine eigene Tätigkeit an dessen Zustand anpasst.

– Collision Avoidance beschreibt einen Mechanismus, der dabei Kollisionen zu vermeiden versucht.

Eine zentrale Rolle bei der Funktionsweise des Zugriffsmechanismus spielt die Zeit zwischen zwei Datenpaketen, der Interframe Space (IFS). Um die Belegung des Mediums zu ermitteln, hört eine sendewillige Station für die IFS-Zeit das Medium ab.

Findet während dieser Zeitspanne keine Kommunikation statt, so ist das Medium mit hoher Wahrscheinlichkeit frei. Der 802.11-Standard definiert verschiedene IFS-Zeiten, die unterschiedliche Prioritätsstufen für den Zugriff widerspiegeln. Dabei gilt: Je kürzer der IFS ist, desto höher ist die Priorität.

Die grundlegende IFS-Zeit heißt die Distributed IFS (DIFS). Die auf DIFS basierende Distributed Coordination Function (DCF) nutzt alle Stationen, um Zugang zum Übertragungsmedium zu bekommen. Der sendewillige Teilnehmer hört zunächst das Medium ab. Bleibt das Medium mindestens für die DIFS-Zeit frei, so kann die Übertragung starten.

Wird das Medium dagegen als belegt erkannt, stellt die Station die Übertragung für eine bestimmte Wartezeit zurück. Die Bestimmung dieser Zeitspanne erfolgt innerhalb des Backoff-Prozesses. Das recht aufwendige Backoff-Verfahren dient dazu, die Wahrscheinlichkeit von Kollisionen soweit wie möglich zu verringern.

Zunächst generiert die Station eine zwischen Null und einem Maximum liegende Pseudo-Zufallszahl. Das gewählte Maximum bezeichnet man als Contention Window (Wettbewerbsfenster). Die Zufallszahl, multipliziert mit einer Zeitschlitzdauer, dient als Backoff-Counter. Solange die Station das Medium als belegt erkennt, bleibt dieser Zähler konstant. Wird das Medium frei, wartet die Station zunächst die DIFS-Zeit ab. Anschließend zählt sie den Backoff-Counter bis Null zurück. Ist nun das Medium noch immer frei, steht dem Senden nichts mehr im Weg.

Der Zugriff auf das Medium erfolgt also per CSMA/CA; hier treten in verschiedenen Situationen Wartezeiten auf:

– IFS,
– DIFS,
– SIFS,
– EIFS.

IFS ist die Wartezeit beim CSMA/CA-Verfahren von WLAN-Clients. Es gibt

– die DIFS, distributed IFS, als Wartezeit zwischen Datenpaketen,
– die SIFS, short IFS, als Wartezeit zwischen einem Datenpaket und seinem Acknowledge,
– die PCF IFS, als Wartezeit eines Point Coordinators, der Zugriffsberechtigungen an WLAN-Clients verteilt,
– die EIFS, extended IFS, als Wartezeit nach einem Frame-Fehler.

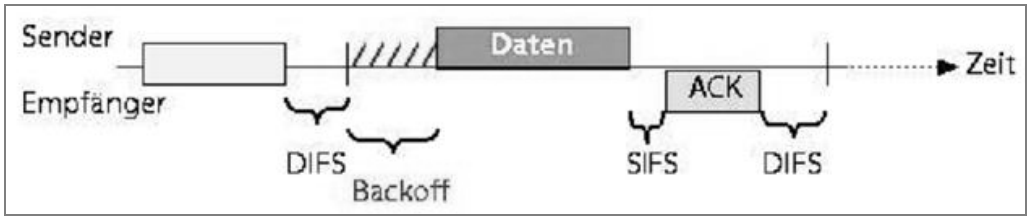


Abb. 5: *Wartezeiten im WLAN*

Möchte eine Station senden und findet das Medium belegt vor, so muss sie eine zufällig lange Backoff-Zeit abwarten. Unterschiedlich lange Inter Frame Spaces (DIFS, SIFS) organisieren den Zugriff auf den Funkkanal.

Weitere Informationen zu CSMA/CA und den Wartezeiten finden Sie unter anderem hier:

– http://www.informatik.fh-nuernberg.de/professors/roth/WS0607/MobileInternet/CSMACA.pdf
– http://forum.fachinformatiker.de/networking-technologies/61569-csma-cd-csma-ca.html
– http://www.jh4all.de/schule/upload/Zugriffsverfahren_fertig.pdf
– http://www.it-infothek.de/fhtw/semester_2/re_od_08.html
– http://www.schorschi.org/dipl/node14.html

Kommen wir nun zu den Betriebsarten im WLAN.

10.4 WLAN-Betriebsarten

WLAN (Wireless LAN, Wireless Local Area Network, ist ein drahtloses funkbasiertes lokales Netzwerk, das dem IEEE 802.11-Standard zugrundeliegt. Im Vergleich zum Kabelnetzwerk (Ethernet) nach IEEE 802.3-Standard gibt es hier keine physikalischen Datenübertragungswege; die am Netzwerk beteiligten Stationen tauschen Datenpakete aus, die sie per Funk versenden.

Die Nutzung kabelloser Kommunikationstechniken ebenso wie die Übertragungsgeschwindigkeiten nehmen von Jahr zu Jahr zu:

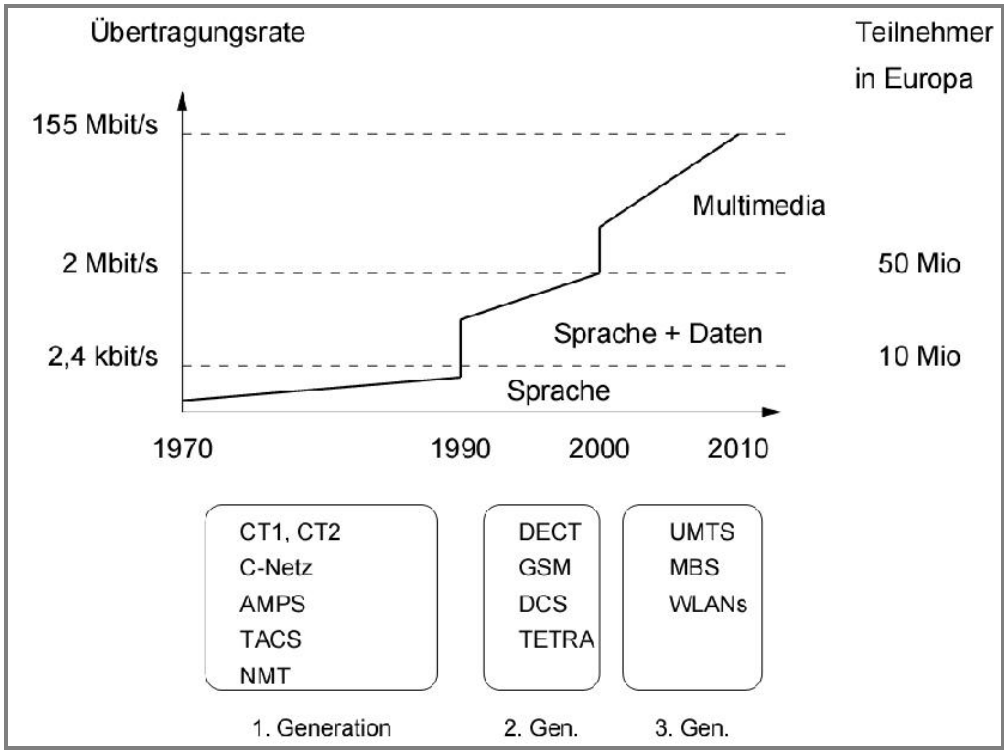


Abb. 6: *Akzeptanz und Geschwindigkeit der kabellosen Kommunikationstechniken*
Quelle: http://wwwspies.informatik.tu-muenchen.de/

Ein solches kabelloses Netzwerk kann je nach Hardware-Ausstattung und den Anforderungen des Betreibers auf verschiedene Weisen aufgebaut bzw. für unterschiedliche Zwecke eingesetzt werden.

Ein funkbasiertes Netzwerk (WLAN) lässt sich

– im Infrastruktur-Modus,
– im Adhoc-Modus sowie
– als Wireless Distribution System (WDS)

realisieren.

10.4.1 Infrastruktur-Modus

Ein Infrastruktur-Netzwerk ist ein WLAN mit mindestens einer Basisstation. Eine solche Basisstation ist ein Access-Point oder Funk-Router, der die Verbindung zum kabelgebundenen Netzwerk herstellt.

Im Infrastruktur-Modus übernimmt ähnlich wie im Mobilfunknetz jeder drahtlose Router (Funkübertragung) bzw. Access-Point[17] Koordinationsaufgaben sowie die Steuerung der Kommunikation der Clients untereinander.

Ein Access-Point sendet in der Regel zehnmal pro Sekunde kleine Datenpakete (Beacons, „Leuchtfeuer") an alle Geräte im Sendebereich[18]. Die Beacons enthalten u. a.

– den Netzwerknamen (Service Set Identifier, SSID[19]),
– eine Liste der unterstützten Übertragungsraten,
– das Verschlüsselungsverfahren.

Dies vereinfacht den Verbindungsaufbau erheblich, da die Clients bereits den Netzwerknamen und die Verschlüsselungsdaten[20] kennen, was für die Verbindung mit dem Access-Point und den anderen Stationen notwendig ist.

Der kontinuierliche Versand der Beacons ermöglicht dem Access-Point die Überwachung der Empfangsqualität[21] – auch dann, wenn über das Netzwerk keine Nutzdaten übertragen werden. Da die Beacons mit sehr geringer Übertragungsrate gesendet werden, ist allerdings durch deren störungsfreie Übertragung noch keine stabile Netzwerk-Verbindung garantiert.

---

17 Informationen zu Funk-Routern/Access-Points bzgl. Funktionsweise, Aufgaben im Netzwerk und Aufbau erhalten Sie im weiteren Verlauf dieser Lerneinheit.

18 Siehe auch http://www.elektronik-kompendium.de/sites/net/0907101.htm, oder http://www.pcwelt.de/index.cfm?pid=1647&pk=36203&p=9.

19 Service Set Identifier (SSID) ist eine aus bis zu 32 alphanumerischen Zeichen bestehende Zeichenfolge, die den Namen des WLAN darstellt. Damit die Clients des WLAN miteinander kommunizieren können, müssen alle Geräte den gleichen SSID verwenden.

20 Genauere Informationen folgen im weiteren Verlauf des Lehrgangs oder vorab unter http://www.wireless-24.de/wlan-einrichten/wlan-verschluesselung/.

21 Informationen zur Verbesserung des Signals finden unter http://www.ovalnets.de/praxis-wlan-empfangsqualitaet-und-reichweite-verbessern.

Nachteil des Infrastruktur-Modus ist die Abhängigkeit von der Basistation: Kommt es hier zu einem Ausfall des Routers (Abschalten oder Stromausfall), dann ist die komplette Kette unterbrochen und es findet kein Netzwerkverkehr mehr statt.

Die folgende Abbildung zeigt ein Wireless LAN, in dem ein einzelner Funk-Router drei mobile Clients verwaltet und die Kommunikation zwischen diesen steuert.

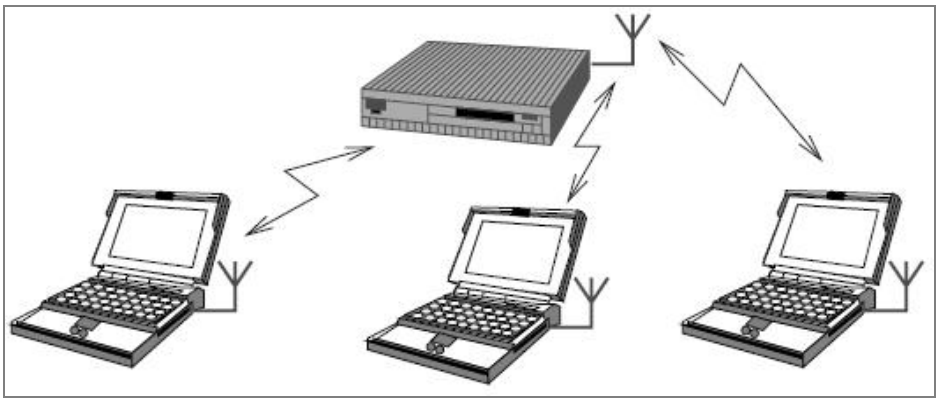


Abb. 7: *Infrastruktur-Modus mit einer Basisstation*
Quelle: http://subs.emis.de

In der folgenden Abbildung sind 3 Basisstationen/Access-Points in einem Infrastruktur-Netzwerk zu sehen.

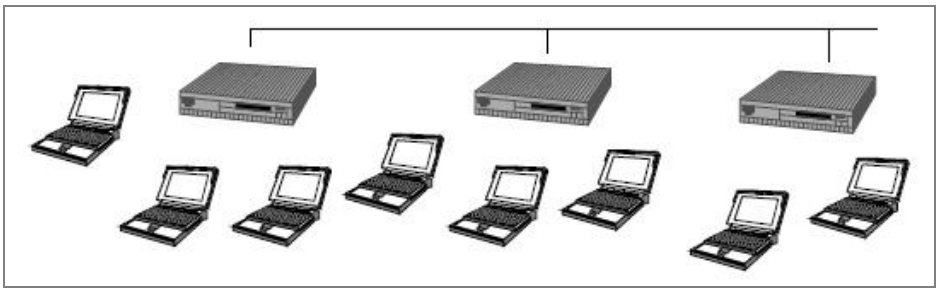


Abb. 8: *Infrastruktur-Modus mit mehreren vernetzten Basisstationen*
Quelle: http://subs.emis.de

Speziell bei größeren Entfernungen zwischen Client und Access-Point ist es wünschenswert, dass die Kommunikation nicht über den Access-Point sondern direkt von Client zu Client möglich ist. Das reduziert einerseits den Netzwerktraffic und andererseits entlastet es den Access-Point erheblich.

Zwar gibt es bereits einen Standard, der diesen Kommunikationsverlauf vorsieht; dieser heißt IEEE 802.11e. Jedoch hat sich dieser bisher nicht durchgesetzt – nahezu kein Access-Point unterstützt diese Norm. Daher hat das IEEE im Jahr 2007 eine Arbeitsgruppe gegründet, welche einen entsprechenden neuen Standard entwerfen soll, den IEEE 802.11z.

Es gibt diesbezüglich schon Entwürfe, allerdings ist die Norm noch nicht veröffentlicht und damit noch kein gültiger Standard. Im Laufe dieser Lerneinheit kommen wir auf diese Thematik noch einmal zurück.

Da im WLAN auf der Sicherungsschicht (2. Schicht des OSI-Modells) dieselben Adressierungstechniken[22] wie im Ethernet zur Anwendung kommen, kann ein Access-Point mit Ethernet-Anschluss (RJ45-Buchse) eine Verbindung zwischen Kabelnetzwerk und Funknetzwerk herstellen.

Ein Client im Ethernet kann folglich nicht unterscheiden, ob er mit einem anderen Ethernet-Client oder über einen Access-Point mit einem WLAN-Client kommuniziert. Der Access-Point hat dabei die Funktion einer Bridge; er übernimmt die Konvertierung bzw. Protokollumwandlung zwischen 802.11-Standard (WLAN) und 802.3-Standard (Ethernet), bildet also eine Brücke zwischen Kabel- und Funknetzwerk.

Im Infrastruktur-Modus dient der Access-Point auch zur Steigerung der Reichweite: Er kann die Funktion eines Repeaters übernehmen, indem er die Pakete der verschiedenen Stationen weiterleitet und dabei die Signalstärke erhöht.

Hier einige weiterführende und vertiefende Links zu diesem Thema

– http://www.virenschutz.info/Infrastruktur-Modus-Wlan-Tutorials-7.html
– http://www.voip-information.de/wlan/wlan-infrastruktur.php
– http://www.html-world.de/program/wlan_4.php

10.4.2 Adhoc-Modus

Neben dem Infrastrukturmodus, in welchem ein WLAN–Router die Steuerung und Kontrolle der Kommuniktion übernimmt, gibt es auch eine WLAN-Betriebsart ohne Router – den Adhoc-Modus:

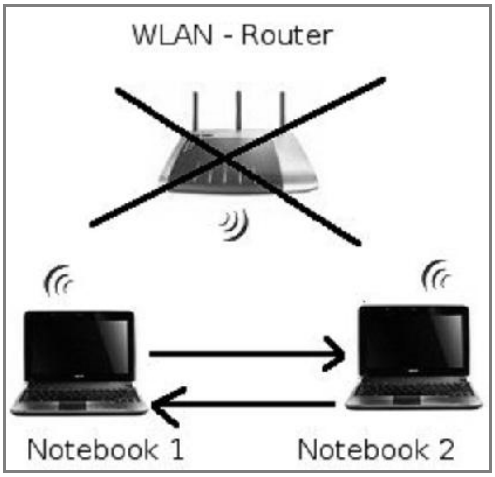


Abb. 9: *Adhoc-WLAN*
Quelle: http://www.heimnetzwerk-und-wlan-hilfe.com

Im Adhoc-Modus kommunizieren zwei oder mehr Clients bzw. Geräte über Funkverbindungen unmittelbar miteinander. Hier ist keine Station besonders

[22] Zur WLAN-Adressierung siehe auch http://telecom.htwm.de/telecom/praktikum/html/wlan/wlan_protokolle1.htm oder https://home.zhaw.ch/~kls/kt/WLAN.pdf.

ausgezeichnet, alle sind gleichwertig (Peer-to-Peer). Es findet nicht wie im Infrastruktur-Modus eine zentrale Koordination/Netzwerksteuerung statt.

Das folgende Bild stellt einen Drucker und einen Laptop dar, zwischen denen eine Adhoc-Verbindung besteht.

Abb. 10: *Adhoc-Vernetzung von Drucker und Laptop*
Quelle: www.linux-magazin.de

Die folgende Abbildung zeigt ein kabelloses Adhoc-Netzwerk bestehend aus 3 mobilen Computern, die per Funk ohne ein zusätzliches Steuergerät direkt miteinander kommunizieren:

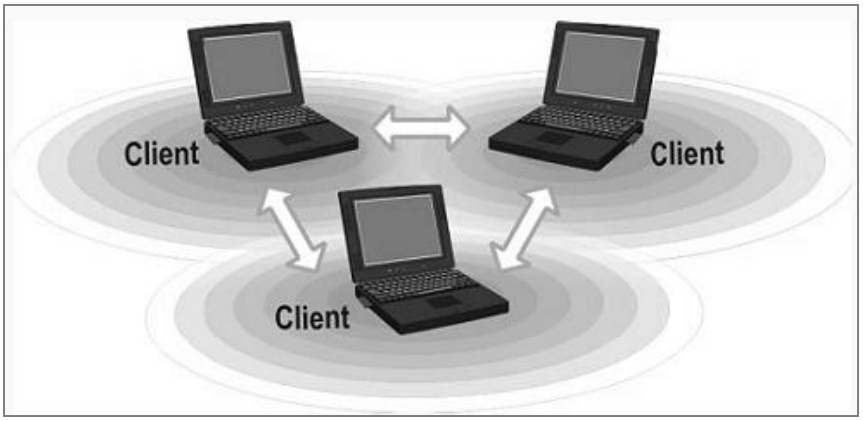


Abb. 11: *Adhoc-Vernetzung mehrerer Mobilcomputer*
Quelle: http://www.stsm.info/dipl/dipl_1.html

Auch im Adhoc-Modus benutzen alle Teilnehmer denselben Netzwerknamen (Service Set Identifier, SSID) und identische Einstellungen für die Verschlüsselung. Da es in einem Adhoc-Netz kein zentrales Vermittlungsgerät (Access-Point) gibt, muss die Koordination von den Endgeräten selbst übernommen werden.

Die Weiterleitung der Datenpakete zwischen den Clients ist nicht vorgesehen und auch nicht ohne weiteres möglich, denn im Adhoc-Modus werden keine Informationen versendet, die den einzelnen Teilnehmern einen Überblick über das Netzwerk geben könnten.

Der Adhoc-Modus eignet sich nur für eine sehr geringe Anzahl Geräte, die sich allerdings aufgrund der begrenzten Reichweite des Funksignals nahe beieinander befinden müssen.

Die Kommunikation der Clients untereinander ist nur möglich, falls

– jedes Gerät eine bestimmte Sendeleistung einhält,
– die Signaldämpfung durch optische oder bauliche Hindernisse hinreichend gering ist,
– die räumliche Entfernung der einzelnen Clients nicht zu groß ist und
– alle Clients auf demselben Funkkanal senden.

Bei zu großer Entfernung zwischen den Clients kommt es zu Kommunikationsstörungen, da einzelne Datenpakete nicht am Zielgerät ankommen.

Möchte man diesen Effekt vermeiden, so muss mindestens ein Gerät im Adhoc-Netzwerk als Gateway fungieren und mit Routing- und ggf. Repeating-Funktionen ausgestattet werden.[23]

Der Adhoc-Modus ist also eine einfache Form eines Funk-Netzwerkes ohne Access-Point, in dem zwei oder mehrere Clients miteinander kommunizieren. Hier verbinden sich die Sende- und Empfangseinheiten der einzelnen Stationen (WLAN-Karten oder Dongles mit externen oder integrierten Antennen) direkt mit einander (Peer-to-Peer). Beachten Sie dabei, dass ein WLAN-Adapter kein Dongle im herkömmlichen Sinn ist.[24]

WLAN-Karte und WLAN-Dongle bzw. –Adapter gehören zur Client-Hardware, auf die wir im weiteren Verlauf dieser Lerneinheit eingehen werden.

Weitere Informationen zum Adhoc-Modus finden Sie unter anderem hier:

– http://de.wikipedia.org/wiki/Adhoc-Netz
– http://www.pc-erfahrung.de/hardware/wireless-lan/wlanfunknetzwerkei.html
– http://www.wireless-lan-test.de/uebersicht-zum-Adhoc-modus.html

[23] Siehe bei Wikipedia http://de.wikipedia.org/wiki/Wireless_Local_Area_Network#Adhoc-Modus

[24] Ein Dongle im herkömmlichen Sinne ist ein Kopierschutzstecker, der auch Hardlock oder Key genannt wird. Derartige Dongles dienen häufig dazu, Software vor unautorisierter Vervielfältigung zu schützen. Sie werden mit der Software ausgeliefert, und müssen auf eine Schnittstelle des Rechners (etwa LPT1 oder USB) aufgesteckt werden. Die Software kontrolliert während des Betriebs regelmäßig, ob der Kopierschutzstecker angeschlossen ist und verweigert bei Nicht-Vorhandensein den Dienst oder ist dann nur eingeschränkt nutzbar. Dongles kommen vor allem in Verbindung mit Software im oberen Preisbereich (mehrere tausend Euro pro Lizenz) und/oder bei leistungsfähigen Serverprogrammen zum Einsatz. Weitere Informationen dazu findet man etwa unter http://de.wikipedia.org/wiki/Dongle.

10.4.3 Wireless Distribution System

Zur Vergrößerung der Reichweite eines Funknetzes oder auch für die Verbindung von Kabelnetzwerken per Funk benötigen Sie eine Wireless Bridge (kabellose Netzüberbrückung). Diese Netzwerkarchitektur wird auch als Bridge-Modus bezeichnet.

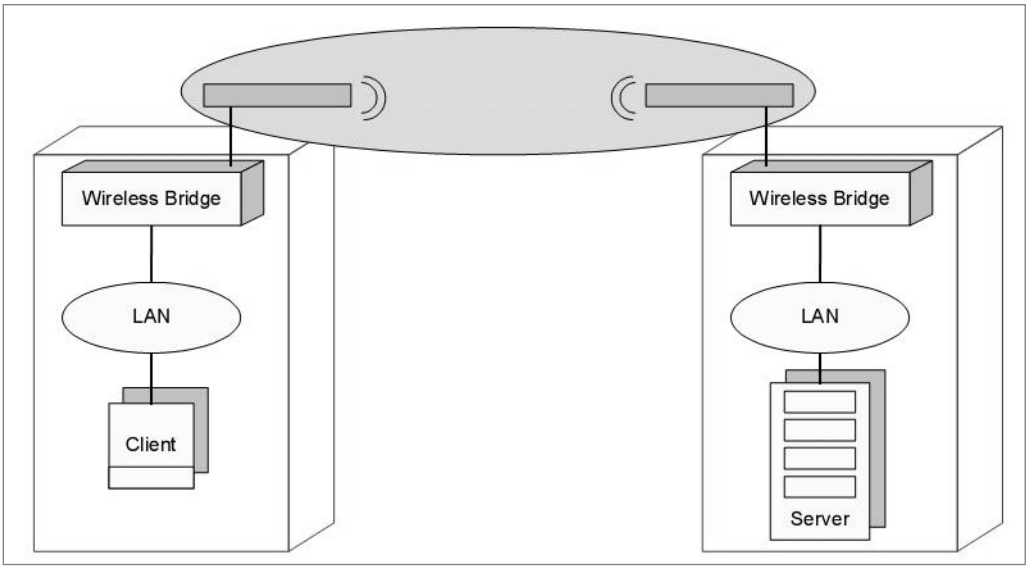


Abb. 12: *Funkverbindung zwischen 2 LANs*

Die folgende Abbildung demonstriert den Aufbau/die Struktur eines Wireless Distribution Systems; Sie sehen hier zwei Infrastrukturnetzwerke, welche über einen Gateway[25] verbunden sind.

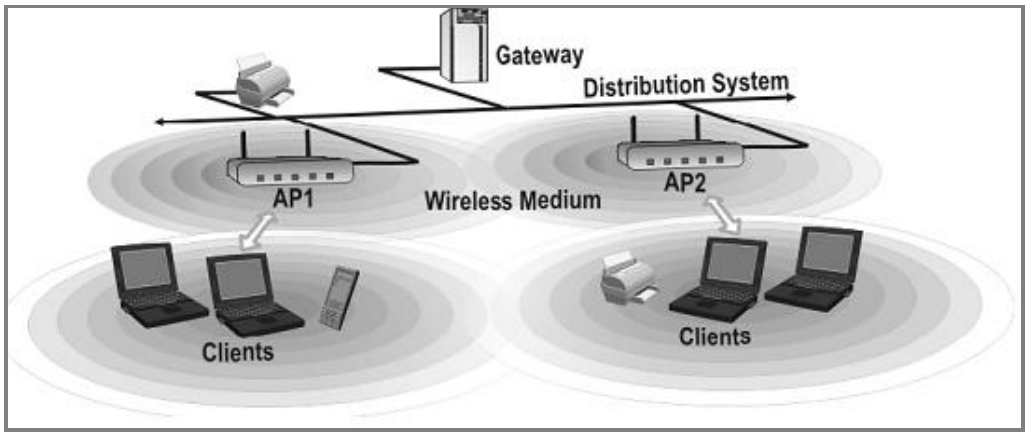


Abb. 13*: WDS-Beispiel*
Quelle: http://www.stsm.info/dipl/dipl_1.html

In einem Wireless Distribution System bzw. Wireless Distributed System (beide Bezeichnungen werden synonym verwendet), kurz WDS, befinden sich mehrere WLAN-Basisstationen (Access-Point), die per Funk miteinander kommunizieren und gemeinsam das Netzwerk kontrollieren. So lässt sich eine größere Netzabdeckung

[25] Der Gateway kann zusätzlich sämtliche Clients der Teilnetze mit einem anderen Netzwerk oder auch mit dem Internet verbinden.

erreichen als mit einem einzigen Access-Point – ohne dass Kabel verlegt werden müssen. [26]

Genau genommen ist ein Wireless Distribution System eine spezielle Erweiterung eines funkbasierten Infrastruktur-Netzwerkes; hier werden mehrere Infrastruktur-Netze miteinander gekoppelt.

Sie kennen jetzt die verschiedenen Architekturen von Funknetzwerken (WLAN). Der folgende Abschnitt setzt sich mit der speziellen WLAN-Hardware auseinander.

10.5 WLAN-Geräte

Alle WLAN-Geräte arbeiten nach dem gleichen Prinzip: Datenpakete werden per Funkwellen statt auf dem Kabelweg übertragen. Sender und Empfänger stellen sich dabei auf einen bestimmten Funkkanal (Band/Spektrum/Bereich für die Frequenz der ausgesendeten Funkwellen) ein, alle anderen Funksignale verwerfen sie.

Das bedeutet, dass sich alle Geräte auf einem bestimmten Funkkanal die Bandbreite, d.h. die insgesamt zur Verfügung stehende Datenübertragungsleistung, teilen – je mehr Nutzer sich also an einem Access-Point anmelden bzw. je mehr Geräte an der Kommunikation im WLAN beteiligt sind, desto geringer ist der Datendurchsatz für die einzelnen Anwender/-innen bzw. jedes einzelne WLAN-Gerät.

Aus diesem Grund sinkt mit zunehmender Anzahl Clients sowohl

– im Adhoc-Netzwerk als auch
– im Infrastruktur-Netzwerk

der Datendurchsatz der einzelnen Verbindungen.

Das Aufrüsten eines solchen Netzwerkes zum WDS durch Zerlegung in mehrere Teilnetze oder das Erweitern um weitere Basisstationen bzw. Access-Points kann die Datenübertragungsraten und auch die Reichweite des Netzwerkes wieder erhöhen.

Der Nutzen eines WLAN steigt und fällt mit der Signalqualität und der damit verbundenen Nettoübertragungsrate.

Die Signalqualität in Funknetzwerk hängt von vielen Faktoren ab; eine entscheidende Rolle spielt/spielen

– die Qualität der Sende- und Empfangsantennen,
– Störsender, die denselben Frequenzbereich wie WLAN nutzen,
– volle Unterstützung der aktuellsten Standards durch alle beteiligten Geräte,
– die Anzahl der Clients, welche sich die Bandbreite teilen,
– die Verschlüsselungstechnik.

[26] Weitere Informationen zu Wireless Distribution Systemen finden Sie bei Wikipedia: http://de.wikipedia.org/wiki/Wireless_Distribution_System

Wie auch im Ethernet gibt es im Funknetzwerk

– Clients,
– Server,
– Verteiler,
– Router,
– Bridges,
– Repeater,
– Netzwerkadapter.

Es handelt sich allerdings vorwiegend um aktive Netzwerkkomponenten, da es im WLAN weder

– Stecker noch
– Verbindungskabel

gibt.

Einzige passive Komponenten sind die Antennen und deren Anschlüsse/Schnittstellen. Allerdings werden diese sehr selten losgelöst sondern eher als zugehörig zur jeweiligen Hardware, wie

– Netzwerkadapter oder
– Access-Point

betrachtet. In den meisten Fällen sind sie fest montiert/integriert und somit ohne Weiteres nicht austauschbar.

Doch speziell welche Hardware kommt im Funknetzwerk zum Einsatz? In den folgenden Abschnitten werden Sie diese Geräte näher kennen lernen.

10.5.1 Client-Hardware

In einem WLAN benötigen Sie pro beteiligten Computer einen WLAN-Adapter, also entweder

– einen WLAN-Dongle mit USB-Schnittstelle,
– eine WLAN-Erweiterungskarte (z. B. mit PCI-Schnittstelle), die auf das Motherboard (Hauptplatine des Computers) aufgesteckt wird,
– eine Steckkarte bzw. Erweiterungskarte für mobile Computer (etwa mit Mini-PCI oder PCMCIA-Schnittstelle) oder
– ein spezielles Motherboard, auf dem bereits ein WLAN-Chipsatz verlötet (integriert) ist.

Übung 1: Ermitteln Sie Hersteller, Typ und Modellbezeichnung Ihres WLAN-Adapters.

Übung 2: Stellen Sie die wichtigsten technischen Eigenschaften Ihres Wireless LAN-Adapters zusammen.

Die folgenden Abbildungen zeigen verschiedene Fabrikate von WLAN-Dongles/-Adaptern mit USB-Schnittstelle. Die kleineren beiden Geräte besitzen eine interne (integrierte) Antenne. Der dritte Dongle (oben rechts) besitzt eine externe Antenne, sein USB-Interface ist durch eine Schutzkappe verdeckt.

Abb. 14: *WLAN-Dongles*

Übung 3:

Welche Vorzüge besitzt ein WLAN-Adapter mit externer Antenne?

Auf dem nächsten Bild sehen Sie einen weiteren Adapter für Funknetzwerke; diese Steckkarte ist PCI-kompatibel und muss in ein Desktop- oder Towergehäuse in einen freien Steckplatz (Slot) des Motherboards eingesetzt werden. Der Adapter besitzt eine externe Antenne und unterstützt den 80211g-Standard.

Abb. 15: *PCI WLAN-Karte (IEEE 802.11g)*

Übung 4:

Der hier dargestellte WLAN-Adapter besitzt eine angeschraubte Antenne. Welche Vorteile besitzt diese gegenüber einer fest verlöteten Sende- bzw. Empfangseinheit?

Was zeichnet einen Dongle bzw. eine WLAN-Karte mit externer Antenne aus? Eine externe Antenne lässt sich gezielter ausrichten. Das Signal wird weniger abgeschirmt bzw. gedämpft, da die Antenne nicht von einem schützenden Gehäuse umgeben ist.

Externe Antennen sind oft leistungsfähiger als interne Antennen, welche nur aus einem winzigen Chip bestehen; auch sind sie in einigen Fällen abschraubbar und damit leicht auszutauschen und gegen ein leistungsfähigeres Modell ersetzen.

Das folgende Bild zeigt einen Wireless Lan-Adapter mit mehreren Antennen; er unterstützt den Standard IEEE 802.11n.

Abb. 16: *PCI WLAN-Karte (IEEE 802.11n)*

Achten Sie beim Kauf eines WLAN-Adapters auf die Antennenanbringung; falls sich die Antenne abschrauben lässt, können Sie diese etwa bei Defekt leicht durch eine andere ersetzen und auch der Austausch gegen eine leistungsstärkere Sende-/Empfangseinheit ist problemlos möglich.

Es gibt auch funktionsgleiche Steckkarten für mobile Computer, die allerdings eine andere Schnittstelle zum Systembus besitzen:

Abb. 17: *WLAN Laptop-Karte mit PCMCIA-Interface*

Die PCMCIA-Schnittstelle ist veraltet und langsam – eine solche WLAN-Karte überträgt im Funknetzwerk etwa 20 MBit/s. Ihre Nachfolge hat die ExpressCard-Schnittstelle angetreten, welche bis zu 2 GBit/s übertragen kann; eine derartige WLAN-Karte ermöglicht netto ca. 150 MBit/s, brutto 300 MBit/s:

Abb: 18: *WLAN-Karte mit ExpressCard-Schnittstelle*

Die hier gezeigten WLAN-Karten besitzen integrierte Antennen zum Senden und Empfangen der Funksignale.

Übung 5:

Welche Vorteile und welche Nachteile besitzen derartige mobile WLAN-Karten gegenüber anderen WLAN-Adaptern?

Die internen Antennen dieser Adapter sind nicht austauschbar. Das Funksignal erfährt durch das Rechnergehäuse oft erhebliche Dämpfung. Andererseits ist die Bauweise des Adapters sehr kompakt. Die Karte wird eingeschoben, ist voll Plug&Play-fähig und bei laufendem System anschließbar; sie muss nicht verschraubt werden, das Rechnergehäuse braucht für Ein- und Ausbau der Karte nicht geöffnet zu werden. Speziell im Falle ExpressCard ist der interne Bus sehr schnell. Die kompakte Karte verursacht wenig Materialeinsatz, ist daher kostengünstig zu produzieren.

Zu den wichtigsten technischen Eigenschaften eines WLAN-Adaptes gehören die Bauweise,

- die Schnittstelle zum Systembus,
- unterstützte Standards,
- seine Anzahl Antennen,
- die Bruttoübertragungsrate,
- technische Ausstattung (etwa Verschlüsselung auf Knopfdruck),
- unterstützte Betriebssysteme,
- Plug & Play-Fähigkeit,
- implementierte Sicherheitsmechanismen.

Übung 6:

Schließen Sie Ihren WLAN-Adapter ordnungsgemäß an Ihren Rechner an und stellen Sie dessen Funktionsfähigkeit her. Beseitigen Sie ggf. Treiberprobleme oder sonstige Konflikte (Gerätemanager).

Zum Betrieb eines WLAN als Adhoc-Netzwerk ist die hier gezeigte und vorgestellte Hardware ausreichend; jede Station benötigt ausschließlich einen WLAN-Adapter.

In einem Infrastruktur-Netzwerk dagegen wird die Kommunikation von einer Basisstation bzw. einem Access-Point gesteuert. Davon handelt der folgende Abschnitt.

10.5.2 Access-Point

Für den Infrastruktur-Modus benötigen Sie zusätzlich zu den Netzwerk-Clients, welche jeweils mit einem externen WLAN-Dongle (USB-Schnittstelle) oder einem anderen WLAN-Adapter ausgestattet sind, noch einen Access-Point, d. h. eine Basisstation für die Steuerung der Kommunikation und für den Zugriff auf das WLAN überhaupt.

Ein solcher Access-Point besitzt die Form einer Box – ähnlich wie ein Verteiler/Switch und auch ein Router im Ethernet; er verfügt zum Senden und Empfangen über eine (oder mehrere) Antenne(n), die entweder

– intern auf der Platine oder
– außen am Gehäuse

angebracht ist/sind. Außerdem besitzt er ein eingebautes oder externes Netzteil und (wie ein Router) Schnittstellen zum Ethernet und Internet (Kabelnetzwerk, WAN).

Innerhalb des Gehäuses (in der Regel handelt es sich um ein Kunststoffgehäuse oder ein Metallgehäuse) befindet sich u.a.

– eine Platine[27] und
– ein Chip mit Betriebsprogramm bzw. Firmware[28].

Übung 7 – 9:

Erarbeiten Sie gemäß Handbuch und auch mit Hilfe von Informationen auf der Website Ihres Access-Point Herstellers, welche Arbeitsschritte für ein Firmware-Update Ihres Access-Point notwendig sind.

Suchen Sie im WWW nach der neuesten Firmware-Version für Ihren Access-Point. Arbeiten Sie die entscheidenden Neuerungen im Vergleich zur vorhandenen Firmware-Version heraus.

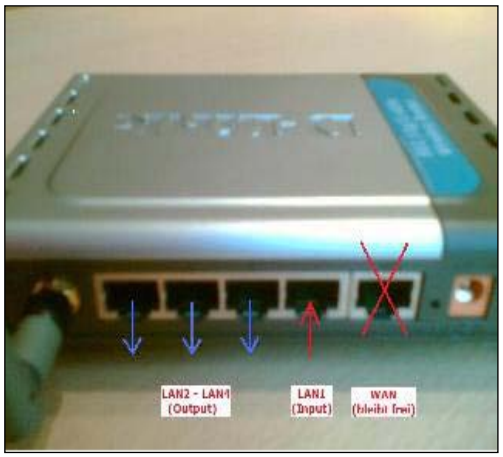
Ermitteln Sie die exakte Modellbezeichnung Ihres Access-Point sowie die Version der Firmware.

[27] Die Platine ist eine kleine Platte aus Kunststoff, auf der winzige elektronische Elemente untergebracht sind. Sie ist ähnlich der Platine, die auf der obigen Abbildung der PCI-WLAN Karte zu sehen ist.

[28] Die Firmware ist ein kleines Programm, das die Funktionen und Prozesse eines Gerätes, wie z. B. eines Routers oder einer Digitalkamera steuert. Die Firmware wird auf einem speziellen fest eingebauten Speicherbaustein innerhalb des Gerätes gespeichert. Die meisten Geräte sind derart ausgelegt, dass die Firmware durch den Anwender selbst bei Bedarf aktualisiert werden kann; dadurch ist es möglich, dass das Gerät neue Funktionalitäten bekommt. Durch eine neue Firmware können zum Beispiel Kompatibilitätsprobleme mit anderen Peripheriegeräten behoben, Sicherheitslücken geschlossen oder höhere Datenübertragungsraten erreicht werden.

Das folgende Bild zeigt einen Access-Point mit Metallgehäuse und einer außen angebrachten (externen) Antenne:

Abb. 19: *Frontansicht eines Access-Point*



Auf der Rückseite des Gerätes befinden sich einige Schnittstellen zum Kabelnetzwerk:
Die außen angebrachte Antenne lässt sich abschrauben und bei Bedarf durch ein leistungsfähigeres Fabrikat ersetzen.

Ein Access-Point arbeitet als Router im WLAN und verteilt die Datenpakete zwischen den einzelnen Stationen. Außerdem dient er ggf. als Brücke (Wireless Bridge) zu einem kabelgebundenen Netzwerk und/oder dem Internet.

Abb. 20: *Rückansicht eines Access-Point*

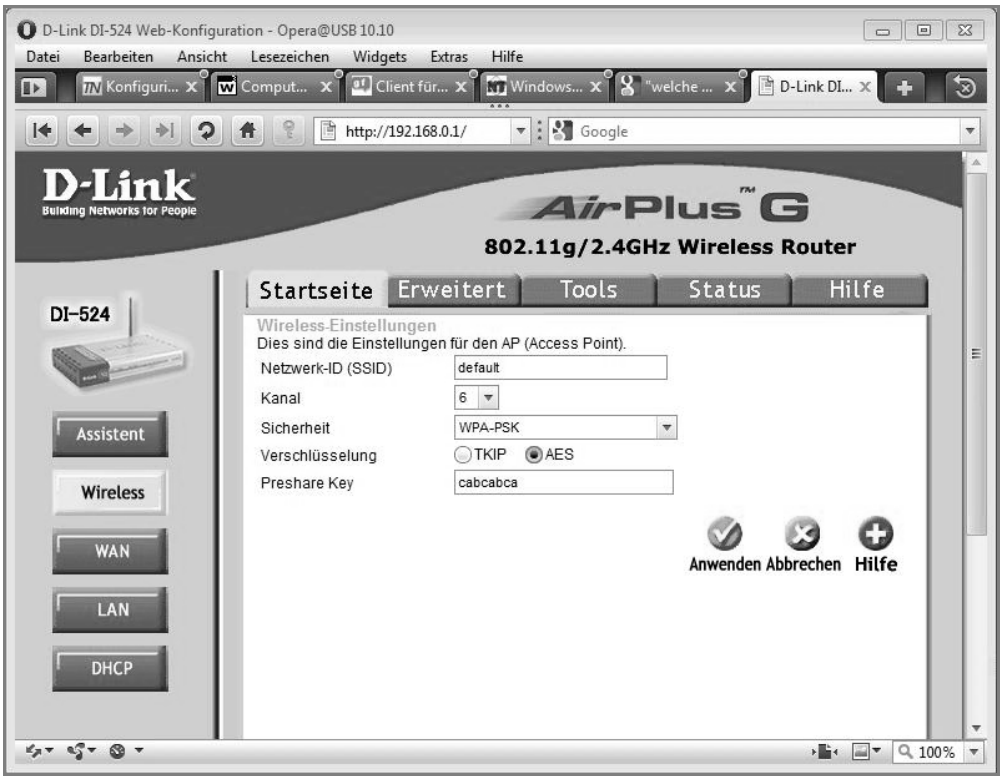


Abb. 21: *Access-Point Konfiguration*

Auf dem Chip des Access-Point befindet sich bei den meisten Produkten ein Konfigurationsprogramm, das es ermöglicht, die Einstellungen des Access-Point zu ändern bzw. an die eigenen Bedürfnisse anzupassen. Unter anderem lassen sich hier Einstellungen für

– DHCP,
– Sicherheit und
– Netzwerk

verändern.

Insbesondere lässt sich hier

– die SSID,
– die interne IP-Adresse im lokalen Netzwerk,
– die Filterung von MAC-Adressen,
– das Zugangskennwort
– der Sendekanal

administrieren.

Viele Hersteller von Computer-Hardware liefern ihre Produkte einschließlich

– Produktbeschreibung,
– Installationsanweisung,
– Handbuch und auch
– Diagnose-Tools

aus, allerdings zum Teil in englischer Sprache. Die beim Kauf eines Access-Points mitgelieferten Informationen liegen oft nicht in gedruckter Form sondern als

– HTML-Dokumente oder
– PDF-Dateien

auf einem CD-Datenträger vor, bei einigen Geräten sind sie lediglich als Download auf der Webseite des Herstellers verfügbar.

Einigen Geräten liegt eine gedruckte Kurzanleitung bei, das vollständige Benutzerhandbuch müssen Sie aus dem WWW downloaden; im Regelfall handelt es sich dabei um eine PDF-Datei, in manchen Fällen liegt eine Offline-Website mit zahlreichen HTM- oder HTML-Dateien und verlinkten Bildern (meistens JPG oder GIF) vor.

Insbesondere das Konfigurationsprogramm präsentiert sich häufig mit englischen Menüs, Meldungen und Hilfetexten. Je nach Modell/Hersteller

– befindet es sich auf dem Chip des Gerätes, so dass Sie es per Browser öffnen und so den Access-Point/das WLAN konfigurieren können,
– liegt es als unter Windows ausführbares Programm vor, welches Sie zunächst auf einem lokalen Computer installieren müssen.

Übung 10:

Ermitteln Sie sämtliche über die reine WLAN-Funktionalität hinausgehende Eigenschaften Ihres Access-Point und stellen Sie diese in einer Liste dar.

Es gibt heute kaum noch Geräte, die reine Access-Point Funktionalität besitzen; die meisten Modelle bieten zahlreiche Zusatzfunktionen an. Mehr dazu erfahren Sie im folgenden Abschnitt.

10.5.3 Kombi-Geräte

Die meisten heute erhältlichen Access-Points sind Multifunktions- bzw. Kombi-Geräte; bei ihnen sind mehrere Funktionalitäten der Gerätetypen

– Router/Switch,
– DSL-Modem,
– Telefonanlage,
– Access-Point

vereint. Durch den Einsatz eines Multifunktionsgerätes verschwindet zumindest ein Teil des Geräte- und Kabelchaos vom Schreibtisch bzw. aus dem Büro.

Ein solcher kompakter WLAN DSL-Router (auch als WLAN-Modem o. ä. bezeichnet) macht es also – je nach Ausstattung bzw. Integration der einzelnen Komponenten – neben der Konfiguration/Verwaltung eines kabellosen Infrastruktur-Netzwerkes möglich,

– ein Kabelnetzwerk mit mehreren Computern aufzubauen,
– eingehende DSL-Signale für das gesamte Netzwerk zur Verfügung zu stellen und Daten in das Internet zu übertragen,
– dass sowohl per Funk als auch per Kabel verbundene Geräte miteinander kommunizieren (Bridge-Funktion).

Besitzt das Gerät zudem eine USB-Schnittstelle (je nach Gerät kann diese vom Typ A oder B sein), so können die Netzwerkteilnehmer bzw. Stationen auf ein angeschlossenes USB-Gerät wie etwa

– externe Festplatte,
– Scanner,
– Drucker,
– Kartenleser,
– USB-Stick

zugreifen.

Manche Geräte besitzen sogar ein oder mehrere Telefonanschlüsse sowie die Funktionalität einer DECT-Basisstation[29]. Eine solche Basisstation ist ein Elektrogerät mit einer Antenne; ist das Gerät mit einer Telefonanschlussdose verbunden, so stellt

[29] Weitere Informationen zum DECT-Standard finden Sie unter
http://de.wikipedia.org/wiki/Digital_Enhanced_Cordless_Telecommunications
http://www.teltarif.de/h/dect.html
http://www.bfs.de/de/bfs/druck/infoblatt/Schnurlos_DECT.html.

es die Verbindung (Bridge) zwischen mobilen Telefongeräten und dem Telefonnetz (Kabelnetz) her.

Je nach Ausstattung des WLAN-Modems und der anzuschließenden Geräte benötigen Sie für das Einbinden zusätzlicher Geräte über die USB-Schnittstelle ggf. Adapterstecker oder zusätzliche Verbindungskabel. Hier ein Überblick über die gebräuchlichsten USB-Anschlüsse:

Abb. 22: *USB-Stecker und Buchse, Typ A*

Abb. 23: *USB-Stecker und Buchse, Typ B*

Beim Kauf eines WLAN-Modems mit USB-Schnittstelle sollten Sie daher darauf achten,

- von welchem Typ der USB-Anschluss ist,
- ob zum Lieferumfang ein USB-Kabel gehört,
- von welcher Art die Schnittstellen der in das Netzwerk einzubindenden Geräte sind,
- ob die Länge des USB-Kabels ausreichend ist,
- welche Stecker/Buchsen an den Enden des evtl. mitgelieferten USB-Kabels angebracht sind.

Fortschrittliche Geräte besitzen mehrere Antennen und sind über einen Touchscreen bedienbar:

Abb. 24: *WLAN-Modem (Hersteller: D-Link)*

Übung 11:

Welche maximale Bruttoübertragungsrate lässt sich bei paralleler Übertragung über alle außen angebrachten Antennen des hier dargestellten Gerätes nach der IEEE 802.11n-Norm erreichen?

Paradebeispiel für ein Kombigerät mit WLAN-Funktionalität ist die Fritz!Box Fon WLAN 7270; sie ist

– WLAN-Router,

– DSL-Modem sowie

– Telefonanlage für Voice over IP (VoIP) und Festnetz

in einem einzigen Gerät – eine wahrhaft funktionsreiche Kommunikationszentrale:

Abb. 25: *Fritz!Box Fon WLAN 7270 (Frontansicht)*

Übung 12:

Die hier abgebildete Fritzbox unterstützt den Draft IEEE 802.11n-Standard. Wie lässt sich die volle 802.11n-Unterstützung erreichen?

Bei diesem Gerät könnte die Kompatibilität zum IEEE 802.11n-Standard durch ein Firmware-Update erreicht werden. Nach diesem Standard sind je Antenne höchstens (brutto) 150 MBit/s erreichbar, also insgesamt 450 MBit pro Sekunde. Dies wird durch die neue Mimo-Technik (Multiple Input Multiple Output) möglich.

Abb. 26: *Fritz!Box Fon WLAN 7270 (Rückansicht)*

Die Fritzbox besitzt – wie die Abbildung zeigt - Schnittstellen für zwei analoge Telefonendgeräte, mit denen man über Internet oder Festnetz telefonieren kann. Je nach Telefonanschluss können die Verbindungen in das Festnetz sowohl über einen analogen als auch über einen ISDN-Telefonanschluss aufgebaut werden.

Die integrierte DECT-Basisstation erlaubt die Anbindung von bis zu sechs DECT-Handgeräten, Anrufbeantworter und Faxfunktion sind integriert.

Zum Anschluss von Computern oder netzwerkfähigen Geräten dienen

– das kabellose WLAN nach Standard 802.11n (Draft 2.0 mit einer Übertragungsrate von brutto 300 MBit/s)[30] und
– vier Ethernet-Schnittstellen.

Außerdem können Sie über den USB-Anschluss periphere USB-Geräte, etwa

– einen Drucker oder
– eine Festplatte

netzwerkweit zur Verfügung stellen.

Im online verfügbaren digitalen „Handbuch“ zu diesem Gerät finden Sie zahlreiche Informationen bzgl.

– Schnittstellen und deren technische Eigenschaften,
– Installation,
– Bedienung,
– Fehlersuche, etc.

Die PDF-Datei steht unter anderem unter

– http://www.avm.de/de/Service/Handbuecher/FRITZBox/Handbuch_FRITZBox_Fon_WLAN_7270.pdf und
– http://www.e-fon.ch/Media/File/manual_FRITZBox_7270.pdf

zum kostenlosen Download bereit.

Es gibt zahlreiche Hersteller von WLAN-Hardware. Aktuelle Informationen finden Sie unter anderem auf den folgenden Webseiten:

Hersteller	Internetpräsenz
Netgear	www.netgear.de
AVM	www.avm.de
Samsung	www.samsung.de
T-Com	www.t-com.de
D-Link	www.d-link.de
Levelone	www.level-one.de

Tab. 5: *Webadressen einiger Hersteller von WLAN-Hardware*

Die (oft scheinbar vergleichbaren) Geräte (Multifunktionshardware, WLAN-Router o. ä.) unterscheiden sich z. T. erheblich voneinander, so zum Beispiel hinsichtlich ihrer USB-Übertragungsrate: Langsame Schnittstellen entsprechen dem USB 1.1-Standard, die breite Masse unterstützt den USB 2.0-Standard. Es ist damit zu rechnen, dass die Hersteller im Zuge der zunehmenden Unterstützung von USB 3.0 durch die aktuellen Motherboards ihre Access-Points in nächster Zeit mit ultraschnellen USB 3.0-Schnittstellen bzw. –Anschlüssen ausstatten werden.

[30] Draft 2.0 (manchmal auch als Pre 802.11n bezeichnet) ist die Vorab-Version des endgültigen später veröffentlichten IEEE 802.11n-Standards. Zahlreiche WLAN-Geräte unterstützen genau diese Spezifikation; einige von ihnen lassen sich allerdings per Firmware-Update auf den neuesten Stand von IEEE 802.11n bringen.

Allerdings ist aufgrund des noch hohen Preises derzeit nicht zu erwarten, dass dem Gerät ein passendes USB 3.0-Kabel beiliegt; dies würde den Preis des Gerätes erheblich vergrößern.

Informationen zu den gültigen USB-Standards finden Sie etwa unter

– http://de.wikipedia.org/wiki/Universal_Serial_Bus
– http://www.tecchannel.de/storage/komponenten/401533/usb_20_highspeed_mit_480_mbit_s/index4.html
– http://diepresse.com/home/techscience/hightech/431237/index.do

10.6 WLAN-Hotspots

Drahtlose Netzwerke (Wireless Local Area Network, WLAN) breiten sich zunehmend aus. So verkaufen sich Notebooks, und seit Neuestem auch Netbooks, die in den meisten Fällen mit WLAN-Karte ausgestattet sind, besser als Desktop-Computer. Sogar die aktuellen Handys besitzen häufig ein WLAN-Modul.

Mobilität hat für Computeranwender/-innen einen hohen Stellenwert bekommen.

Auch privat nimmt die Anzahl der kabelgebundenen Netzwerke ab, unterstützt durch die steigenden Verkäufe der Router mit WLAN-Funktionen. Auch steigt die Anzahl öffentlicher Drahtlos-Netzwerke (Hotspots), die in

– Flughäfen,
– Universitäten,
– Firmen,
– Cafés,
– Zügen, etc.

eingerichtet sind.

Ein Hotspot ist ein Funknetzwerk, welches

– frei und ungeschützt für alle oder
– per Passwort/Authentifizierung für einen bestimmten Personenkreis (Kunden, Geschäftspartner, …)

zugänglich ist.

Technisch gesehen ist ein Hotspot ein Wireless Distribution System (WDS), welches je nach Flächendeckung/Reichweite aus wenigen bis hin zu Tausenden Access-Points bestehen kann.

Im World Wide Web gibt es zahlreiche Informationen zu diesem Thema, etwa

– http://de.wikipedia.org/wiki/Hot_Spot_(WLAN)
– http://www.computerbild.de/artikel/cb-Tests-DSL-WLAN-Per-Hotspot-drahtlos-ins-Internet-1899499.html
– http://www.anschlussbereit.de/hotspot.html

– http://www.its05.de/computerwissen-computerhilfe/pc-netzwerk/hotspot/hotspot.html
– http://www.hotspot-server.eu/index-de.html

Wo befinden sich die öffentlichen Internetzugänge genau? Auf der Webseite http://mobileaccess.de finden Sie eine Liste von Hotspots in Deutschland, der Schweiz und Österreich. Sie erfahren dort auch im Detail, wie der Zugang zu dem jeweiligen Netz konfiguriert werden muss.

Aber auch

– Handys,
– Smartphones,
– PDAs, usw.

werden zunehmend – durch Integration entsprechender Hardware-Schnittstellen - mit der Möglichkeit ausgestattet, einen Internetzugang zu nutzen. Die Benutzer/Innen sollen so die Möglichkeit erhalten, nicht nur zu Hause sondern überall ortsunabhängig eine Online-Verbindung herstellen zu können.

Es lässt sich also ein deutlicher Trend hin zu Mobilität und Online-Kommunikation feststellen:

– Zu jeder Zeit,
– an jedem Ort.

Im Mobilfunkbereich ist es selbstverständlich geworden:

– Überall können wir mit unserem Handy oder Smartphone eine Gesprächsverbindung zu anderen herstellen.
– Internet per Handy ist mittlerweile kostengünstig und nahezu flächendeckend in Deutschland verfügbar.

Die Verbindung zum jeweiligen Netz wird durch lokale Sendestationen ermöglicht, die zum Mobilfunknetz eines

– lokal,
– regional/landesweit oder
– global

agierenden Anbieters gehören.

Wenn wir bei einer bestehenden Verbindung unsere Position verändern, so findet ein automatischer Netzwechsel statt; überall – auch außerhalb unseres Heimbereiches – können wir eine Netz-Verbindung herstellen.

Zwar werden täglich zahlreiche Mobilcomputer mit WLAN-Adapter verkauft, jedoch ist deren Mobilität in Bezug auf die Internetverbindung sehr stark eingeschränkt.

Denn: Sowohl ein privates WLAN als auch ein öffentlicher Internetzugang (Hotspot) besitzt eine begrenzte Reichweite. Spätestens bei Überschreiten einer bestimmten Entfernung zum Access-Point (Sie verlassen dabei die Funkzelle) ist die Verbindung unterbrochen. Es sei denn, es ist ein Wireless Distribution System eingerichtet, welches die Flächendeckung des Netzwerks vergrößert.

Wenn Sie sich außerhalb der Reichweite Ihres Access-Point/Ihres Funknetzwerkes befinden, ist die Verbindung (ohne Roaming) unterbrochen. Falls

– Ihr neuer Standort sich innerhalb eines Funknetzwerks (WLAN) befindet und

– Sie Ihre Netzwerkeinstellungen anpassen,

können Sie sich erneut verbinden (sofern Sie die Verbindungsdaten kennen).

Wünschenswert ist sicherlich eine Fortsetzung der aktuellen Sitzung/Online-Verbindung und eine nahtlose Übernahme in das neue Netz, ohne dass Sie irgendwelche Anpassungen Ihrer Netzwerkkonfiguration vornehmen müssen.

Dabei ist nichts wirklich unmöglich: Im ICE von Hamburg nach München können Sie störungsfrei surfen. Ohne Kabel.

Die Voraussetzung dafür wird etwa durch die WiMax-Technik geschaffen, auf die wir im Laufe dieser Lerneinheit genauer eingehen werden.

WLANs besitzen zwar aufgrund ihres lokalen Charakters räumliche Grenzen, lassen sich aber trotzdem in ihrer Reichweite per WDS erweitern. In einem WDS geschieht die Übernahme der Verbindung von Access-Point zu Access-Point durch Roaming. Davon handelt der folgende Abschnitt.

10.7 WLAN-Roaming

Erstreckt sich ein WLAN über eine größere Fläche, so reicht ein Access-Point in der Regel nicht aus. Um den gesamten Bereich funktechnisch abzudecken, muss man mehrere Access-Points platzieren.

Wenn sich die Funkbereiche der Access-Points gegenseitig ein klein wenig überschneiden, dann kann sich der Client zwischen den Access-Points bewegen, ohne dass die Netzwerkverbindung unterbrochen wird. Dieser Sachverhalt heißt Roaming.

Für die Umsetzung gibt es mehrere Verfahren:

1. ESSID - Extended Service Set Identifier
   Am Einfachsten lässt sich WLAN-Roaming realisieren, indem Sie alle Access-Points mit der gleichen SSID ausstatten. Dazu müssen die Access-Points die erweiterte Form der SSID unterstützen: ESSID (Extended Service Set Identifier). Wichtig ist, dass Sie den Access-Points unterschiedliche Kanäle zugewiesen haben, sonst überlagern sich die Funkverbindungen gegenseitig und es kommt keine Verbindung zu Stande.
2. WLAN-Roaming über IEEE 802.11f (IAAP)
   Die Access-Points tauschen sich über das IAPP (Inter Access Point Protocol)[31]

[31] Mit dem Inter Access-Point Protokoll ist in WLANs eine standardisierte Kommunikation zwischen den Access-Points möglich, die über Bridges miteinander verbunden sind. Das IAPP, das in der Norm IEEE 802.11f beschrieben ist, standardisiert das Roaming mobiler Clients über mehrere WLAN-Zellen hinweg. Durch IAPP soll die Interoperabilität von Access-Points verschiedener Hersteller verbessert werden, so dass proprietäre Lösungen überflüssig sind. Siehe dazu z. B. http://www.itwissen.info/definition/lexikon/inter-access-

über die angemeldeten Clients aus. So können sie die Verbindung ohne Unterbrechung übernehmen. Im gesamten Netz darf nur ein DHCP-Server installiert sein. Die Access-Points dürfen dabei nur als **DHCP Relay-Agents** fungieren.[32]

3. Erweiterung einer WLAN-Umgebung durch WDS-Roaming
   Im Repeating-Modus[33] ist es in einem WDS den WLAN-fähigen Endgeräten möglich, sich mit einem beliebigen Access-Point zu verbinden und Daten zu übertragen. Die Access-Points, die im Regelfall kabellos miteinander verbunden sind, ermitteln dabei untereinander die beste Route zum zentralen Gateway, welches die Verbindung zum Internet herstellt.

Mit der Roaming-Funktion kann sich ein Nutzer frei am gesamten Standort bewegen, ohne die Verbindung zum Internet zu verlieren, bzw. beim Wechsel des Access-Points die Verbindung neu herstellen zu müssen.

Weitere Informationen zum Thema Roaming finden Sie u. a. hier:

– http://www.bundesnetzagentur.de/enid/International_Roaming/Was_ist_Roaming_2pd.html
– http://www.elektronik-kompendium.de/sites/net/1407081.htm
– http://hilfe.telekom.de/hsp/cms/content/HSP/de/3378/faq-1003690

10.8 WLAN Schwachstellen

Für WLAN stehen zwei Frequenzbereiche zur Verfügung: Der eine Bereich liegt um 2,4 GHz, der andere um 5 GHz.

Beide Frequenzbereiche sind weltweit lizenzfrei nutzbar. Lediglich für grundstücksübergreifende Netzwerke oder Outdoor-Netze ist eine kostenfreie Registrierung bei der Regulierungsbehörde für Telekommunikation und Post (RegTP) notwendig[34].

---

point-protocol-IAPP-IAPP-Protokoll.html oder auch http://www.galileocomputing.de/glossar/gp/anzeige-10850/FirstLetter-I?GalileoSession=08720581A4ZZC--d0Bg

[32] Ein DHCP-Relay Agent leitet DHCP-Meldungen zwischen DHCP-Clients und DHCP-Servern in verschiedenen IP-Netzwerken weiter. Der Access-Point besitzt also keine DHCP-Server Funktionalität, sondern er vermittelt die DHCP-Kommunkation. Siehe dazu etwa http://technet.microsoft.com/de-de/library/cc783103(WS.10).aspx

[33] Im Repeating-Modus (Point-to-Multipoint, WDS) werden mehrere Access-Points miteinander verbunden, und zusätzlich können sich Clients, etwa Notebooks, verbinden. Zu den Modi siehe etwa http://www.wireless-lan-test.de/tipps-zu-wds-und-repeating.html

[34] Die Regulierungsbehörde für Post und Telekommunikation (RegTP) war bis zum 12.07.2005 der Name einer Bundesoberbehörde im Geschäftsbereich des Bundesministeriums für Wirtschaft. Mit dem Inkrafttreten des Gesetzes zur Neuregelung des Energiewirtschaftsrechts wurde die RegTP in Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA) umbenannt.

Das bedeutet, dass auf privatem Grund und Boden keine Gebühren bezahlt werden müssen, jedoch in diesen Frequenzbereichen noch weitere Anwendungen/Geräte senden und empfangen; dies kann zu gegenseitigen Störungen führen.

Insbesondere das ISM-Frequenzband (Industrial, Scientific, Medicine) um 2,4 GHz wird für Anwendungen in

– Industrie,
– Wissenschaft und
– Medizin

intensiv genutzt.[35]

In diesem Frequenzspektrum um 2,4 GHz konkurrieren viele Standards und proprietäre Funktechniken der unterschiedlichsten Hersteller und Anwendungen. Auch Geräte des täglichen Gebrauchs, z. B.

– Mikrowellenherde,
– Funkfernbedienungen und
– AV-Funksysteme[36]

gehören dazu.

Die Realisierbarkeit eines Funknetzwerks nach IEEE 802.11 hängt also maßgeblich von der Nutzung anderer Sendegeräte ab, die in Reichweite dieses Frequenzspektrum nutzen.

Schaut man sich die Angaben der Hersteller und Händler zur Übertragungsgeschwindigkeit ihrer Produkte an und vergleicht die Werte, die man damit in der Praxis erreicht, so erkennt man, dass die Bruttodatenraten, wie sie auf den Produktverpackungen angegeben sind, in der Praxis nie erreicht werden. Die Bruttodatenraten sind nicht einmal unter optimalen Bedingungen (Sichtkontakt zwischen Sender und Empfänger) und bei kurzen Entfernungen zu erreichen.

Je nach

– Umgebungsbedingungen,
– Anzahl der teilnehmenden Stationen und
– deren Entfernung

---

[35] Als ISM-Bänder (Industrial, Scientific and Medical Band) werden Frequenzbereiche bezeichnet, die durch Hochfrequenz-Geräte in Industrie, Wissenschaft, Medizin sowie in häuslichen und ähnlichen Bereichen genutzt werden können. Entsprechende ISM-Geräte wie Mikrowellenherde und medizinische Geräte zur Kurzwellenbestrahlung benötigen dabei nur eine allgemeine Zulassung. Die ISM-Bänder sind durch die Internationale Fernmeldeunion weitestgehend festgelegt. Einige ISM-Bänder werden auch für Audio- und Videoübertragungen, Datenübertragungen wie WLAN oder Bluetooth verwendet, ohne dass es für diese Nutzung einer Einzel-Frequenzzuweisung bedarf. Diese sind allerdings keine ISM-Anwendungen und unterliegen eigenen Bestimmungen. Durch die gemeinsame Nutzung kann es in den besonders häufig genutzten Bändern, wie etwa dem 2,4-GHz-Band zu Störungen zwischen verschiedenen Geräten kommen. Die Nutzung dieser Frequenzbereiche sowohl für ISM-Zwecke als auch für Funkanwendungen ist in Allgemeinzuteilungen geregelt, welche auf der Website der Bundesnetzagentur www.bundesnetzagentur.de eingesehen werden können.

[36] Ein solches Funkübertragungssystem überträgt Video- und Tonsignale drahtlos im ganzen Haus. Sogar die Infrarot-Signale üblicher Fernbedienungen werden ebenso per Funk in der Gegenrichtung übertragen. Ein Set besteht aus einem Funksender (2,4 GHz-Bereich) und einer Empfangsstation.

erreicht man nur einen Bruchteil der beworbenen maximalen Datenübertragungsgeschwindigkeit. Obwohl Wireless LAN protokollunabhängig arbeitet, können sich Probleme in der Praxis mit einigen Protokollen und Anwendungen ergeben. Ausschlaggebende Faktoren sind

– die höhere Bitfehlerrate (Bit-Error Rate, BER) und
– die größere Verzögerung bei der Übertragung von Daten.

Es liegt in der Natur eines Wireless LAN, dass die zur Übertragung benötigte Zeit länger ist als im drahtgebundenen LAN. Ein einfacher Ping[37] hat im drahtgebundenen LAN eine Round-Trip Time[38] von weniger als einer Millisekunde. Im Wireless LAN liegt die Zeit für einen Ping bei bis zu vier Millisekunden.
Anwendungen, die eine kurze Verzögerungszeit zwischen Senden und Empfangen (Delay) benötigen, zeigen bei der Funkübertragung unter Umständen Funktionsdefizite.

Im Laufe dieser Lerneinheit haben Sie einen guten Überblick über das WLAN von heute bekommen; durch internationale Standards sind

– Schnittstellen,
– Zugriff auf das Medium,
– Datenübertragungsraten,
– Sicherheit,
– Frequenzkanäle,
– Roaming

und vieles mehr geregelt.

Doch welche WLAN-Entwicklungen sind für die nahe Zukunft zu erwarten?

10.9 Das WLAN der Zukunft

Ebenso wie Ethernet und die Informationstechnik als Ganzes soll sich auch WLAN stetig verbessern. Es gibt mehrere

– Gremien und auch
– Interessengruppen,

welche sich mit der Weiterentwicklung der Datenübertragung in Funknetzwerken beschäftigen und bei der Ausarbeitung neuer Standards mitwirken.

---

[37] Schon in früheren Lerneinheiten haben wir das Ping-Signal behandelt: Ping ist ein Dienst von TCP/IP, mit dem man testen kann, ob zwei Geräte im TCP/IP Netzwerk sich miteinander verbinden können.

[38] Sie erinnern sich: Unter Round-Trip Time (RTT) oder Round-Trip Delay (RTD) versteht man die Reaktionszeit eines kompletten Netzwerks. Es ist die Zeitspanne, die erforderlich ist, um ein Signal von einer Quelle über das Netzwerk zum Empfänger zu senden und die Antwort des Empfängers wiederum über das Netzwerk zurück zum Sender zu transportieren. Die Round-Trip Time wird in einigen Routing-Algorithmen bei der Bestimmung der optimalen Route berücksichtigt.

Zu diesen gehört unter anderem das IEEE, welches bereits zahlreiche Normen herausgebracht hat.

Der zukünftige WLAN-Standard könnte IEEE 802.11ad heißen. IEEE 802.11ad ist derzeit kein fertiger Standard, sondern befindet sich noch in der Bearbeitungsphase. Angedacht ist ein WLAN mit Übertragungsgeschwindigkeiten im Gigabit-Bereich.

Da in den bisher genutzten Frequenzbereichen bei 2,4 und 5 GHz keine ausreichend große Bandbreite erreichbar ist, ist in der Norm IEEE 802.11ad ein Frequenzwechsel auf 60 GHz vorgesehen.

Im 60 GHz-Bereich stehen, je nach nationaler Regulierung, 4 bis 7 GHz Gesamtbandbreite zur Verfügung. Damit würde man mehrere Gigabit pro Sekunde an Bruttodatenrate erreichen.

Allerdings ist die Signaldämpfung bei 60 GHz sehr hoch. So eignet sich das zukünftige Gigabit-WLAN nur für die drahtlose (Direkt-)Verbindung zwischen zwei Geräten (Adhoc-Netzwerk). Zum Beispiel lässt sich Gigabit-WLAN einsetzen, um hochauflösende Bilder oder Videos von einem Speicher (z. B. einem Kartenleser) zu einem Anzeigegerät (beispielsweise einem Beamer) zu übertragen.

In vielen Fällen würde die Nettodatenrate kaum höher als in einem WLAN nach IEEE 802.11n-Standard sein, daher wird sich das IEEE hier sicherlich noch einiges einfallen lassen.

Diese Technik ist mit Ultra Wideband-Techniken[39], wie

– Wireless HDMI[40] und
– Wireless USB[41]

vergleichbar.

Eine weitere in Arbeit befindliche Norm ist die IEEE 802.11z.

Das IEEE strebt mit der Entwicklung seiner Norm 802.11z einen Standard (Direct Link Setup, DLS) an, der Verbindungen zwischen WLAN-Geräten im Infrastruktur-Modus ohne Umweg über einen Access-Point ermöglicht. Bisher gibt es Direct Link Setup nur bei Access-Points, die der Norm IEEE 802.11e entsprechen. Die Unterstützung von IEEE 802.11e ist aber nicht weit verbreitet.

---

[39] Ultra Wideband ist eine gegen Störungen relativ unempfindliche Funktechnik, die z. B. in Autosensoren eingesetzt wird, um mit äußerster Genauigkeit Distanzen zu messen. Siehe dazu etwa http://atmvs1.informatik.tu-muenchen.de/Members/baumgaru/seminare/ss06-dlnetzwerke/UWB_Ausarbeitung.pdf

[40] Wireless HD funkt im weltweit lizenzfreien Bereich von 60 GHz; es verbindet Fernseher, DVD- und Bluray-Player, Set-Top-Boxen, Kameras, Spielkonsolen und andere Geräte aus dem Bereich der Unterhaltungselektronik miteinander über kurze Entfernungen. Künftige Generationen sollen Bandbreiten von bis zu 20 GBit/s erreichen. Dabei werden die Daten verschlüsselt übertragen. Alle via Wireless HD verbundenen Geräte sollen sich durch eine gemeinsame Fernbedienung steuern lassen. Siehe etwa http://www.golem.de/0801/56770.html

[41] Bei Wireless USB werden Peripherie-Geräte ähnlich wie bei Bluetooth per Funk mit dem Computer verbunden. Siehe etwa http://www.computerwoche.de/netzwerke/mobile-wireless/599781/ oder auch http://www.tecchannel.de/netzwerk/wlan/1739328/wireless_usb_ergaenzt_wlan_und_blueto oth_technologie/

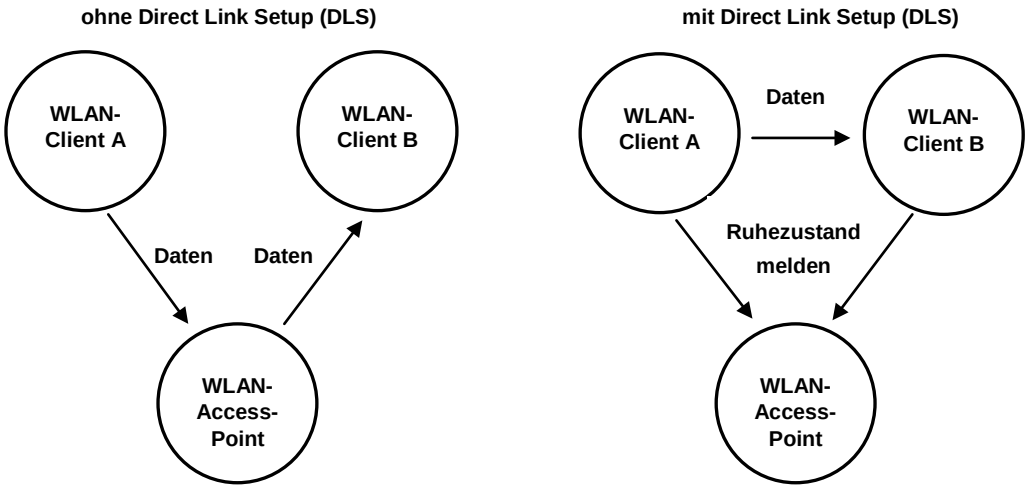


Abb. 27: *Kommunikation ohne/mit Direct Link Setup*

DLS sieht vor, dass für eine direkte Verbindung zwischen zwei WLAN-Geräten keine Vermittlung bzw. Unterstützung durch einen Access-Point notwendig ist. Bei der Aushandlung von DLS verpacken die beteiligten Stationen ihre Datenpakete in spezielle Ethernet-Frames. Der Access-Point leitet auch diese wie gewohnt weiter, bekommt aber ansonsten vom DLS-Aufbau der Stationen nichts mit.

Zur Initiierung der DLS-Session signalisieren die beteiligten WLAN-Geräte dem Access-Point einen vorläufigen Ruhezustand. Infolgedessen speichert der Access-Point temporär für diese Stationen eingehende Datenpakete von anderen (unbeteiligten) WLAN-Geräten.

Parallel dazu wechseln die Stationen auf einen anderen Funkkanal und tauschen dort ihre Daten direkt miteinander aus. Während einer Session melden sich die beteiligten Stationen in regelmäßigen Intervallen wieder beim Access-Point an, um sich eventuell aufgelaufene Datenpakete zukommen zu lassen.

Kommen wir nun zu Bluetooth, einem weiteren kabellosen Übertragungsverfahren.

10.10 Bluetooth

10.10.1 Hardware/Geräte

Bluetooth ist ein Verfahren für die mobile kabellose Kommunikation verschiedenster Geräte auf kurzen Strecken bis zu einer Entfernung von etwa 100 Metern. Es wird hauptsächlich in der persönlichen Informations- und Kommunikationstechnik eingesetzt.

Der Name „Bluetooth“ stammt vom dänischen Wikingerkönig Harald Blatand (genannt Blauzahn), der einst vor über 1000 Jahren die dänischen Provinzen zu einem Königreich vereinigte. Außerdem hat der Name scheinbar auch mit der Dominanz von skandinavischen Technologieunternehmen (Nokia, Ericsson) in der Kommunikations-elektronik zu tun.

Bluetooth wird beispielsweise bei der Vernetzung bzw. dem Datenaustausch zwischen

– Handys,
– Laptops oder
– persönlichen Organizern (PDAs)

verwendet.

Bluetooth-Geräte sind untereinander über das Service Discovery Protocol verbunden. Das **Service Discovery Protocol** (SDP) gehört zu den Bluetooth-Kernprotokollen. Das Protokoll dient der Erkennung der Bluetooth-fähigen Geräte untereinander, damit diese miteinander kommunizieren können.

Über dieses Protokoll werden die Dienstinformationen der einzelnen Geräte ermittelt. Mit diesen werden die Verbindungen zwischen den Bluetooth-Geräten eingerichtet und alle für die Datenübertragung relevanten Informationen übermittelt.

In einem Bluetooth-Netzwerk gibt es keine speziellen Verteiler oder Steuergeräte, diese Funktion wird von den Endgeräten selbst übernommen.

Auch hardware- bzw. ausstattungstechnisch gibt es nicht viel zu beachten, die beteiligten Geräte müssen lediglich einen Bluetooth-Chip besitzen. Bei vielen Geräten ist dieser fest auf der Hauptplatine verlötet/integriert.

Die gegenwärtig auf dem europäischen Markt befindliche bzw. unmittelbar vor der Einführung stehende Palette von Bluetooth-Produkten ist enorm groß. Bluetooth-Module sind oft schon ab Werk in Geräten wie

– Notebooks,
– Kameras,
– Computerperipherie,
– Mobiltelefonen,
– Freisprecheinrichtungen für Mobiltelefone (Headsets),
– Palmtops, usw.

integriert.

Bluetooth-Fähigkeit lässt sich auch nachrüsten, beispielsweise durch unterschiedliche Einsteckkarten für PC und Notebook, sowie extern für alle denkbaren EDV-Peripheriegeräte durch einen Dongle mit USB-Schnittstelle:

Abb. 28: *Bluetooth-Dongle*

Abb. 29: *Bluetooth Mini-Adapter*

Neben internen und externen Modulen sind auch Bluetooth Access-Points erhältlich, durch welche die Anbindung eines Bluetooth-Netzwerkes an ein größeres Local Area Network möglich wird.

In Bezug auf ihre Reichweite kann man Bluetooth-Geräte in Gruppen einteilen, die sich in ihrer Sendeleistung unterscheiden.

– Geräte der Klasse 1 übertragen mit maximal 100 Milliwatt Leistung (etwa 100 Meter Reichweite).
– Geräte der Klasse 2 besitzen eine maximale Leistung von 2,5 Milliwatt (etwa 50 Meter Reichweite).
– Geräte der Klasse 3 senden mit maximal 1 Milliwatt Sendeleistung (etwa 10 Meter Reichweite).

Viele Geräte, beispielsweise Mobiltelefone, die mit anderen Mobiltelefonen oder Headsets über Bluetooth kommunizieren, müssen deshalb nur der schwächsten Klasse angehören, da keine hohe Reichweite für diese Bluetooth-Verbindungen notwendig ist. In vielen Fällen können nur Geräte, die zur selben Klasse gehören, miteinander kommunizieren.

10.10.2 Architekturen

In einem Bluetooth-Netzwerk sind wie schon im WLAN verschiedene Architekturen bzw. Anordnungen der einzelnen Geräte möglich.

Die direkt miteinander über SDP vernetzten Bluetooth-Geräte bilden ein **Piconet(z)** (Kleinverbund elektronischer Geräte), über das

– Videos,
– Sprache,
– Text oder
– Bilder

ausgetauscht werden.

Ein solches Piconetz kann aus bis zu acht Geräten bestehen, von denen eines die Rolle des Master übernimmt, die restlichen sieben als Slave geschaltet sind.

So kann ein Benutzer z. B. sämtliche seiner persönlichen elektronischen Geräte miteinander verbinden.

Bestehen bereits mehrere Piconetze, dann können diese sich zu einem **Scatternet(z)** ebenfalls verbinden. So wird die Kommunikation zwischen Geräten verschiedener Benutzer oder Benutzergruppen möglich.

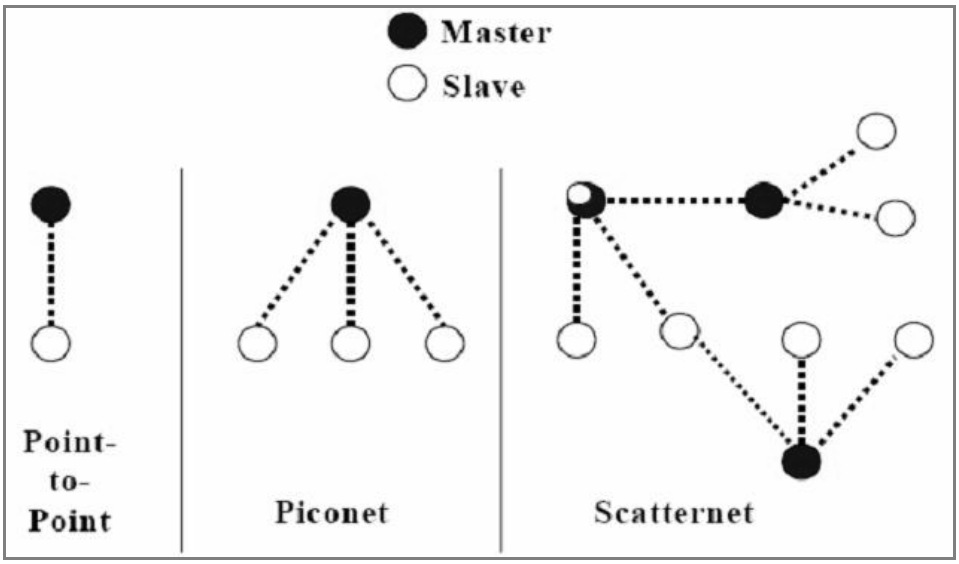


Abb. 30: *Bluetooth-Netze*

Die Abbildung zeigt drei Situationen:

– Direktverbindung (Point-to-Point),

– sternförmige Vernetzung (Piconet),

– verbundene Sternnetze (Scatternet).

Bei einer Point-to-Point Verbindung übernimmt ein Gerät die Funktion des Master, das andere Gerät fungiert als Slave. Die Point-to-Point Verbindung entspricht dem Adhoc-Modus beim WLAN.

Im Piconet gibt es einen Master, der die Funktion eines zentralen Verteilers übernimmt; es liegt also eine Sternstruktur vor – jeder Slave sendet an den Master, der die Daten an das Zielgerät weiter leitet. Ein Piconet ist vergleichbar mit dem Infrastruktur-Modus beim WLAN; allerdings wird im Piconet keine spezielle Basisstation benötigt, sondern die Funktion des Master übernimmt ein an der Kommunikation beteiligtes Gerät.

Im Scatternet gibt es mehrere Piconets. In jedem Piconet gibt es einen Master, die Verbindung von Piconet zu Piconet wird durch ein Slave-Gerät hergestellt, welches beiden Netzen angehört. Je nach Netzstruktur und Position der Geräte kann auch – wie aus der obigen Abbildung ersichtlich ist – ein einziges Gerät mehrere verschiedene Funktionen übernehmen: Es arbeitet in dem anderen Netz als zentraler Verteiler (Master), stellt aber trotzdem die Verbindung zum anderen Piconet her (Slave-Funktionalität).

Die Kommunikation im Scatternet erfolgt ausschließlich über den Master, die unmittelbare Kommunikation zwischen zwei Slaves ist nicht möglich. Da sich die Teilnehmer im Netz permanent ändern können, ist das Piconet auf Grund der Bewegungsfreiheit der Geräte ein dynamisches Kommunikationsnetzwerk.

Bei Bluetooth ist keine Infrastruktur notwendig, um eine Kommunikation zwischen den einzelnen Geräten zu ermöglichen und ein Netzwerk zu bilden.

Hier sehen Sie ein weiteres Beispiel für die Vernetzung von Kommunikationsgeräten per Bluetooth:

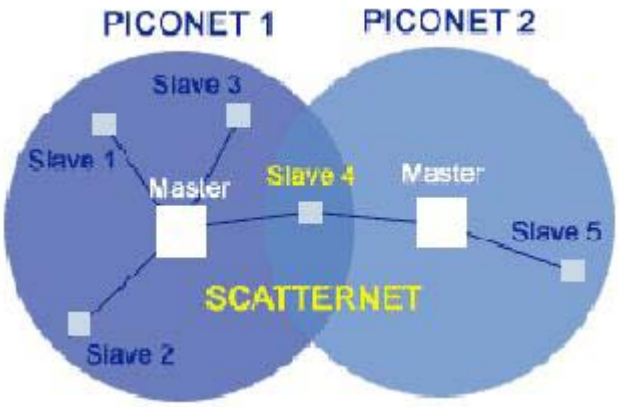


Abb. 31: *Vernetzte Bluetooth-Geräte nach www.tecchannel.de*

In einem Scatternet schließen sich mehrere Piconetze zusammen; die Verbindung läuft jeweils über einen gemeinsamen Slave, wie die Abbildung zeigt. Die Architektur des Scatternet ist ähnlich der eines Wireless Distribution Systems beim Wireless LAN.

10.10.3 Die Standards

Die Datenübertragung und Vernetzung über Bluetooth wird wie auch im Ethernet und bei WLAN durch Standards geregelt.

Die Übertragungsgeschwindigkeit in einem Netzwerk nach dem Standard Bluetooth 1.0 lag bei bis zu einem Megabit in der Sekunde. Bei einer asymmetrischen Datenübertragung verteilte sich die Leitungskapazität auf

– Download (max. 723 Kilobit/s) und

– Upload (bis zu 57,6 Kilobit/s).

Bei symmetrischer Übertragung war je Kanal eine maximale Übertragungsrate von 432,6 Kilobit/s möglich. [42]

Die Spezifikation der Bluetooth 2.0-Version lässt zu, dass Daten durch EDR (Enhanced Data Rate)[43] maximal etwa dreimal so schnell übertragen werden können, wobei sich die beteiligten Geräte die verfügbare Bandbreite teilen müssen (Shared Medium). Das erinnert uns an die Anfänge des Ethernet.

[42] Zur Spezifikation von Bluetooth 1.0 siehe http://www.thewirelessdirectory.com/Bluetooth-Overview/Bluetooth-Specification.htm

[43] Damit das etablierte Bluetooth nicht gleich wieder veraltet, wurde die EDR-Technik (Enhanced Data Rate) entwickelt und in Bluetooth mit der Version 2.0 integriert. Durch EDR profitieren die Anwendungen vom schnelleren Übertragungskanal. Somit bekommen mehrere parallele Verbindungen genügend Kapazität, ohne dass Übertragungsverzögerungen auftreten. Siehe etwa http://www.areamobile.de/news/7010-neuer-bluetooth-standard-2-1-edr

Bluetooth unterstützt die Übertragung von Multimedia-Inforrmationen (Sprache, Text, Bilder, Videos, …). Eine Verschlüsselung der transportierten Daten wurde mit dem Bluetooth 2.0-Standard möglich.[44]

Im April 2009 wurde der Standad Bluetooth 3.0 verabschiedet. Dieser sieht eine maximale Übertragungsrate von 24 MBit/s vor sowie die Unterstützung von WLAN durch kompatible Geräte. [45] Erste Handys und Kleingeräte sind noch relativ teuer.

Auch die 4. Spezifikation ist schon in Arbeit. Das Motto ist:

– Mehr Reichweite,
– mehr Tempo,
– mehr Stabilität.[46]

Bluetooth-Geräte bekommen von ihrem Hersteller eine weltweit eindeutige 48 Bit-Adresse zugewiesen, die mit der MAC-Adresse einer Netzwerkkarte vergleichbar ist. So ist es nahezu unmöglich, dass es zwischen einzelnen Geräten zu Störungen kommt oder die Geräte sich gegenseitig abhören.

10.10.4 Die Technik

Die Vermeidung von Störungen durch Signale anderer Anwendungen erreicht man bei Bluetooth durch ein Baseband-Protokoll; dieses steuert, dass die Trägerfrequenz nicht konstant bleibt, sondern in einer zeitlichen Abfolge verschiedene Werte aus einer festen Menge von Frequenzen annimmt.

Ein Gerät, das eine Nachricht empfangen soll, muss mit dem Sender synchronisiert sein und genau die gleiche Sprungfolge für die Trägerfrequenz verwenden. Nur Nachrichten, die diesen Fingerabdruck tragen, können von den Teilnehmern eines Bluetooth-Netzes empfangen werden, Signale anderer Quellen filtern sie heraus. Die Daten schließlich werden der Sprungfolge durch eine binäre Frequenzmodulation angehängt.

Für die Verbindung per Bluetooth stehen folgende Techniken zur Verfügung:

– SCO = Synchronous Connection-Oriented Link und
– ACL = Asynchronous Connection-Less Link.

Beim Einsatz einer

– synchronen,
– verbindungsorientierten und
– leitungsvermittelten

---

[44] Informationen zu Bluetooth 2 finden Sie etwa hier: http://www.radio-electronics.com/info/wireless/bluetooth/bluetooth_edr.php

[45] Zum 3.0-Standard von Bluetooth siehe http://www.elektronik-kompendium.de/sites/kom/1405151.htm

[46] Zu den neuen 4.0 Spezifikationen siehe http://www.teltarif.de/bluetooth-4-0-sig-spezifikation/news/36924.html

Übertragung spricht man von einer SCO-Verbindung (synchronous connection-oriented). Diese ist eine symmetrische Punkt-zu-Punkt Verbindung zwischen einem Master und genau einem Slave in einem Piconet. Dabei kann der Master bis zu drei SCO-Links gleichzeitig unterstützen. Slaves unterstützen zwei SCO-Links gleichzeitig zu verschiedenen Mastern. Für das Senden ist ein fester Zeittakt definiert, innerhalb dessen eine Übertragung erfolgen darf. [47]

Bluetooth kann in einem asynchronen Modus Pakete übertragen. Reservierte Zeitfenster ermöglichen bei Bluetooth-Übertragung einen Vollduplex-Betrieb, bei dem Kommunikationspartner zur selben Zeit senden und empfangen dürfen.

Die **ACL-Verbindung** (asynchronous connectionless link) ist eine

– asynchrone,

– verbindungslose und

– paketorientierte

Verbindung; sie stellt eine Punkt-zu-Multipunkt Verbindung zwischen dem Master und allen aktiven Slaves in einem Piconet dar (Sterntopologie). Dabei stehen bis zu 7 Kanäle in einem Piconet zur Verfügung.

Zwischen einem Slave und einem Master kann jeweils nur eine ACL-Verbindung bestehen. Slaves können bei diesem Verbindungstyp nur Daten senden, wenn der Master dies anordnet. Da kein fester Zeittakt vereinbart ist, darf nur eine bestimmte Anzahl Zeichen gesendet werden.

Das letzte übertragene Zeichen stellt das Stopp-Signal dar. Es ist keine Reservierung der Slots (Zeitintervalle) für die Übertragung notwendig. Verloren gegangene Pakete werden wiederholt versendet.

10.10.5 Die Frequenzen vom Bluetooth

Der von Bluetooth genutzte Frequenzbereich von 2,402 bis 2,4835 GHz wird in Deutschland in 79 logische Kanäle von jeweils 1 MHz Bandbreite aufgeteilt. Zwischen diesen 79 Kanälen können Bluetooth-Geräte während einer Datenübertragung flexibel springen, also ihre Sendefrequenz wechseln. Die Kanäle werden ca. 1600 Mal pro Sekunde gewechselt. Das Zufallszahlenprinzip, welches dazu verwandt wird, wird zuvor von den miteinander kommunizierenden Geräten vereinbart. Gibt es partielle Störungen im ISM-Band, so können diese durch das Frequenzsprungverfahren (Frequenzhopping) bis zu einem gewissen Grad kompensiert werden.

Bei einer Bluetooth-Verbindung wird das Frequenzband durch das Frequenzsprungverfahren wesentlich effektiver genutzt als bei WLAN-Vernetzung. Erkennt ein Gerät im Laufe der Kommunikation eine Störung, dann

– sendet es einen bestimmten Pseudocode, so dass die beiden Stationen die Sendefrequenz wechseln oder

– es startet einen weiteren Übertragungsversuch.

---

[47] Zur SCO-Verbindung siehe etwa http://telecom.htwm.de/bluetooth/bluetooth/physikal.htm.

Damit Sender und Empfänger zur gleichen Zeit auf den selben Kanal umschalten, wird ein **Hop-Key** verwendet[48]. Seit der Bluetooth-Version 1.2 ist es möglich, dass einzelne ausgelastete Kanäle durch das adaptive Frequenz-Hopping[49] in der Sprungsequenz nicht berücksichtigt werden.

Mit Hilfe des Frequenzsprungverfahrens und des adaptiven Frequenz-Hopping wird die Empfindlichkeit gegenüber Störungen deutlich reduziert. Bluetooth eignet sich damit vor allem für Applikationen, die durch eine zyklische und echtzeitfähige Übertragung von wenigen Steuersignalen in einer störanfälligen Umgebung über eine geringe Entfernung gekennzeichnet sind.

Innerhalb des ISM-Bereiches verwenden verschiedene Regionen bzw. Länder verschiedene individuelle Frequenzbereiche:

Region	Frequenz in GHz	Nutzbare Kanäle
USA	2,4002 – 2,4835	79
Europa	2,4002 – 2,4835	79
Frankreich	2,4465 – 2,4835	27
Spanien	2,4450 – 2,4750	35
Japan	2,4710 – 2,4970	23

Tab.6: *Bluetooth-Kanäle in verschiedenen Ländern*

Bluetooth verwendet in Deutschland 79 verschiedene Kanäle, durch Frequenzhopping ist eine hohe Stör- und Abhörsicherheit gewährleistet.

10.10.6 Sicherheit

Eingebaute Fehlerkorrekturverfahren sorgen im Störungsfalle dafür, dass zu übertragende Daten abgesichert werden. Dadurch sinkt im Einsatzfall zwar die effektive Datenübertragungsrate, in so einem Fall wird jedoch die Notwendigkeit einer zusätzlichen Übertragungssicherung höher bewertet als das Erreichen der maximal erreichbaren Übertragungsbandbreite.

Bluetooth besitzt einen Verschlüsselungsmechanismus, der auf Basis von symmetrischer Verschlüsselung arbeitet. Damit eine Bluetooth-Kommunikation erfolgen kann, ist es notwendig, dass alle beteiligten Bluetooth-Geräte sich kennen.

---

[48] Ein Hop-Key ist eine vereinbarte Zeichenfolge, nach der sich beide Stationen auf einem anderen Kanal wieder treffen.

[49] Das ISM-Band im 2,4-GHz-Frequenzbereich wird unter anderem auch von WLAN verwendet. Da sich die verschiedenen Funktechniken gegenseitig beeinträchtigen, die Leistungsfähigkeit reduzieren und Interferenzen bilden, hat man mit dem adaptiven Frequenzsprungverfahren (Adaptive Frequence Hopping, AFH) eine Technik entwickelt, die bei gegenseitiger Beeinträchtigung aktiviert werden kann. Mit der AFH-Technik wird die Frequenzsprung-Sequenz dann geändert, wenn ein WLAN die Übertragungsfrequenzen von Bluetooth beeinträchtigt. Das AFH-Verfahren gehört seit der Version 1.2 zum Bluetooth-Standard. Siehe
etwa http://www.itwissen.info/definition/lexikon/adaptive-frequency-hopping-AFH.html

Dies wird mit dem so genannten **Pairing** erreicht, bei dem nach anderen Geräten gesucht wird und nach Abfrage eines Schlüssels das jeweilige Gerät als vertrauenswürdig eingestuft wird, worauf mit ihm dann Daten ausgetauscht werden können. Diese Autorisationskennung dient dann gleichzeitig auch der Verschlüsselung.

Zusätzlich gibt es drei **Security-Level**:

– Non-secure, Mode 1,
– Service-Level („untrusted/trusted devices“), Mode 2,
– Link-Level, Mode 3.

In der ersten Stufe gibt es keine Sicherheitsmechanismen, die Geräte erkennen sich und können ohne Authentifizierung[50] miteinander kommunizieren. Für den Mode 2 sind flexible Zugriffe bei unterschiedlichen Sicherheitsanforderungen vorgesehen. Die Geräte erkennen sich, können aber ohne Authentifizierung keine Verbindung zueinander herstellen.

In Mode 3 werden die Sicherungsprozeduren bereits beim Verbindungsaufbau initialisiert, der mit dem Verbindungsschlüssel ausgeführt wird. Darüber hinaus dient dieser 128 Bit lange Schlüssel zur Generierung des Sitzungsschlüssels oder Link Key, mit dem auch die Geräte authentifiziert werden.

Beim Link Key kann es sich um einen Kombinationsschlüssel handeln, gewonnen aus der Schlüsselkombination zweier Geräte. Es kann sich aber auch

– um einen Geräteschlüssel,
– um einen temporären Schlüssel, der nur für die aktuelle Sitzung benutzt werden kann, oder
– um einen Initialisierungs-Schlüssel zum Schutz der Verbindungsparameter bei der Übertragung handeln.

Bei Bluetooth gibt es nahezu keine Anonymität, wie das im Internet der Fall ist. Dies ist durch die räumliche Nähe der miteinander verbundenen Geräte bedingt.

---

[50] Authentifizierung bedeutet aufgaben- und benutzerabhängige Zugangs- und/oder Zugriffsberechtigung. Die Authentifizierung hat den Zweck, Systemfunktionen vor Missbrauch zu schützen. Bei der Kommunikation stellt die Authentifizierung sicher, dass der Kommunikationspartner auch derjenige ist, für den er sich ausgibt.

Bei der Authentifizierung wird zwischen einseitiger und gegenseitiger Authentifizierung unterschieden. In der Praxis wird meistens die einseitige Authentifizierung verwendet, wobei beispielsweise beim Login der Benutzer sein Passwort eingibt und damit nachweist, dass er wirklich der angegebene Benutzer ist. Als Sicherheitsdienst für die einseitige Identifikation dient der Empfängernachweis, durch den die Benutzer-Identität und damit auch die Benutzungsberechtigung gegenüber dem System nachgewiesen wird. Dazu dienen hauptsächlich Passwörter, persönliche ID-Nummern, kryptografische Techniken sowie Magnet- oder Chip-Ausweiskarten. Eine strenge Authentifizierung kann mit der Vergabe von Einmalpasswörtern (OTP = One Time Passwords) erfolgen.

Darüber hinaus gibt es Authentisierungssysteme, die mit biometrischen Daten arbeiten, und Mehrfaktorsysteme, die unter anderem auf so genannte USB-Token (Stecker oder Dongle, der zur persönlichen Authentifizierung des Anwenders dient) setzen.

Sicherer als die einseitige Authentifizierung ist die gegenseitige, bei der alle Kommunikationspartner ihre Identität beweisen müssen, bevor untereinander vertrauliche Daten ausgetauscht werden. So sollte beispielsweise beim Abheben von Bargeld an einem Terminal (Ein-/Ausgabegerät) dieses vor Eingabe der PIN beweisen, dass es sich bei dem Gerät um ein echtes Geldausgabegerät handelt und nicht um einen Nachbau oder eine Konsole, welche nur die eingegebenen Daten aufzeichnet (Keylogging).

10.10.7 Anwendung

Trotzdem Bluetooth im 2,4 GHz-Band den gleichen Frequenzbereich wie WLAN nutzt, konkurrieren beide Verfahren nicht direkt miteinander, sondern ergänzen sich durch ihre Zielsetzung. Während WLAN eher dazu gedacht ist, das Netzwerkkabel abzulösen, ersetzt Bluetooth in erster Linie Kabel für EDV- und Telefonzubehör.

Bluetooth wird also vornehmlich in Umgebungen verwendet, in denen nicht sehr viele Anschlussoptionen notwendig sind, sondern es hauptsächlich wichtig ist, dass kleine Datenmengen zuverlässig von einem zum anderen (Kleinst-)Gerät übertragen werden können.

Bluetooth ist weniger ein Netzwerkprotokoll, sondern vielmehr eine End-to-End Schnittstelle, die ursprünglich als reiner Kabelersatz vorgesehen war.

Die Märkte der Einsatzgebiete

– Unterhaltungselektronik und
– Telekommunikation

erzielen gute Umsätze.

Über Bluetooth können die Anwender/-innen auch eine Anbindung an das Internet herstellen. So lassen sich über Gateways z. B. MP3-Dateien aus dem weltweiten Datennetz auf das Handy laden.

Mit Bluetooth sollten die Verbindungskabel zwischen Peripheriegeräten und Computer der Vergangenheit angehören. Das ist inzwischen Realität: Man kann mit Bluetooth

– Maus,
– Tastatur,
– MP3-Player,
– Modem,
– Webcam,
– digitale Bilderrahmen,
– Drucker,
– Mobiltelefon,
– PDA,
– Organizer und
– Videokamera

an einen Rechner anbinden und serielle Kabelverbindungen ersetzen.

Es gibt auch Audio-Anwendungen, z. B.

– drahtlose Kopfhörer oder
– Freisprecheinrichtungen für Mobiltelefone.

Auch im Heimbereich hält Bluetooth Einzug. So kann man beispielsweise über eine im Eingangsbereich des Hauses installierte Kamera jeden Zutritt am Computerbildschirm beobachten oder einen in einem anderen Raum befindlichen Drucker nutzen – das Ganze ist möglich, ohne ein einziges Kabel zu verlegen. Auch die Fernsteuerung von Haushaltsgeräten über das Handy lässt sich realisieren.

Im Bürobereich kann Bluetooth eingesetzt werden, um elektronische Visitenkarten auszutauschen oder auch um eine Präsentation auf einem mit dem Laptop verbundenen Projektor auszugeben.

Hier einige für Bluetooth typische Anwendungen:

– Handys mit Bluetooth-Chip schalten am Arbeitsplatz automatisch auf den kostenlosen Betrieb im firmeninternen Telefonnetz um und funktionieren zu Hause als Schnurlosapparate im Festnetz.
– Die Teilnehmer einer Konferenz brauchen ihre Notebooks nur einzuschalten, um sie miteinander zu verbinden.
– Der Referent braucht kein Kabel, wenn er den Projektor per Bluetooth an einen PC anschließt.
– Eine E-Mail, die der Anwender im Flugzeug auf seinem Notebook verfasst, wird abgeschickt, sobald er nach der Landung sein Handy auf Standby schaltet.
– Der PDA des Außendienstmitarbeiters tauscht selbstständig über Bluetooth mit dem PC im Büro Informationen aus und aktualisiert seine Daten.

Die Nutzung dieser Technologie ist aus medizinischer Sicht ebenso unbedenklich wie die von Wireless LAN.

Die Chancen für die Zukunft von Bluetooth stehen äußerst gut, da seitens der Industrie großes Interesse an dieser Technologie besteht. Tausende von Firmen arbeiten am Bluetooth-Standard (www.bluetooth.com).

Hier noch mal eine Übersicht der wichtigsten Eigenschaften der Bluetooth-Technologie:

– Es ist ein offener Standard im Bereich 2,4 GHz.
– Es handelt sich um eine Spreizspektrum-Technik mit 1600 Frequenzsprüngen je Sekunde (Frequenz-Hopping).
– Bluetooth-Geräte senden auf 79 Frequenzen (2,402–2,4835 GHz).
– Die Bluetooth-Technologie ermöglicht Reichweiten bis zu 100 m.
– Bluetooth stellt 3 Sicherheitslevels zur Verfügung.
– Die Datenrate beträgt maximal 24 MBit/s.
– Im gleichen Frequenzbereich senden auch andere Geräte, daher besteht die Möglichkeit gegenseitiger Störungen.

10.11 Die Funkstandards im Vergleich

Die drahtlosen Übertragungstechnologien

– Bluetooth,
– Infrarot,
– WLAN

unterscheiden sich zum Teil stark. So zum Beispiel in der Art der Ausbreitung der Signale oder in der Geschwindigkeit, mit der Informationen vom Sender zum Empfänger transportiert werden.

Der größte Unterschied im Übertragungsprinzip besteht darin, dass sich die Signale bei WLAN und Bluetooth über Funkwellen ausbreiten, bei Infrarot hingegen über Lichtwellen. WLAN und Bluetooth senden in einem bestimmten Frequenzbereich, Infrarot mit bestimmten Wellenlängen.

Zur Veranschaulichung dient die folgende Tabelle:

Technik	Frequenzbereich	Wellenlänge
Bluetooth	2,4000 GHz – 2,4835 GHz	---
WLAN	2,4000 GHz – 2,4835 GHz 5,7250 GHz – 5,8500 GHz	---
Infrarot	---	780 nm – 1 mm

Tab. 7: *Drahtlose Techniken*

Große Unterschiede können auch bei der Reichweite der einzelnen Technologien nachgewiesen werden. Die Richtwerte sind:

– bei WLAN wenige km,
– bei Bluetooth max. 10 m bzw. 100 m bei Verstärkung,
– bei Infrarot wenige Meter.

Bluetooth und WLAN funken also im gleichen Frequenzbereich, eignen sich jedoch für unterschiedliche Einsatzbereiche: Bluetooth ist erste Wahl, wenn Sie zwei (Klein-)Geräte verbinden möchten, die sich in unmittelbarer Nähe zueinander befinden, etwa

– Handys,
– PDAs,
– Headsets.

Zu jeder der genannten Technologien wurden auch entsprechende Anwendungen beschrieben. Es dürfte hierbei auffallen, dass man das, wofür die eine Technologie verwendet werden soll, in vielen Fällen auch mit einer anderen realisieren kann. Doch die genaue Art der zu lösenden Aufgabe entscheidet oft letztendlich über die Art der Problemlösung. Dabei spielen sicherlich auch Installationsaufwand sowie die Kosten für

– Geräte,
– Material und
– Software

eine Rolle.

Beispiel:

Wenn Sie einen Drucker drahtlos an einen PC anschließen möchten, so ist das theoretisch mit allen drei Übertragungstechnologien möglich. Praktisch ist es nicht ganz so einfach. Befindet sich der Drucker beispielsweise viele Stockwerke höher oder tiefer oder gar in einem anderen Gebäudetrakt als der Rechner, so kommt meist nur Wireless LAN für die Realisierung dieses Vorhabens in Frage. Steht er jedoch direkt im benachbarten Zimmer, so kann er im Normalfall auch mit Bluetooth erreicht werden. Infrarot ist nur dann tauglich, wenn sich der Drucker im gleichen Raum befindet und eine direkte Sichtverbindung vorhanden ist, über die die Daten vom Sender zum Empfänger gelangen.

Aufgrund der Dominanz von Wireless-LAN bei kabellosen Verbindungen besitzt Bluetooth wenig Bedeutung. Neben den günstigen Anschaffungskosten für die benötigte Hardware kann Bluetooth bei der Einrichtung und den Einsatzmöglichkeiten überzeugen. So können Sie etwa Peripheriegeräte wie Drucker kabellos anschließen oder Verbindungen zwischen

– PDA,
– Notebook und
– Handy

realisieren.

Damit sich Bluetooth-Geräte für bestimmte Aufgaben einsetzen lassen, besitzen sie Profile zur Verbindungsaufnahme und zum Abgleich der Funktionen. Es gibt rund 30 Profile für sehr unterschiedliche Einsatzzwecke.

Die Kommunikation funktioniert ausschließlich zwischen Geräten mit den gleichen Profilen. Die Profile bauen teilweise aufeinander auf: So müssen alle Bluetooth-Komponenten GAP (Generic Access Profile) beherrschen, um überhaupt miteinander in Kontakt treten zu können. Per SDAP (Service Discovery Application Profile) fragen Bluetooth-Geräte die jeweiligen Profile ab.

Die Bluetooth-Funktechnik eignet sich für den drahtlosen Datenaustausch zwischen mehreren Geräten, die je nach Profil zwischen 10 Metern und 100 Metern entfernt sein können.

Auf Basis einer Master/Slave-Techik gibt es Empfänger und Sender – die meisten Bluetooth-Geräte lassen sich sowohl als Slave als auch als Master einsetzen. Die Nachteile von Bluetooth gegenüber Wireless LAN sind

– geringe Datenrate und
– geringe Reichweite.

Die Datenrate von Bluetooth eignet sich eher für Anwendungen mit seltenem Datenaustausch in meist kleinem Umfang. So bildet Bluetooth keine Konkurrenz zu Wireless-LANs. Die wesentlichen Bluetooth-Applikationen bestehen aus unternehmenseigenen Anwendungen wie

– Messaging,
– Knowledge Management,
– Datenbankabfragen sowie
– Zugang zum Internet.

Besonders kleine Geräte profitieren von der geringen Größe und dem moderaten Stromverbrauch der Bluetooth-Chips.

Dagegen kommt WLAN immer dort zum Einsatz, wo Sie bislang ein fest verkabeltes Netzwerk benötigten. Für ein WLAN sprechen besonders das höhere Tempo und die bessere Reichweite.

Während der Entwicklung des WLAN-Standards IEEE 802.11 und der von Bluetooth haben sich viele Gemeinsamkeiten herausgestellt. Beide Funkstandards übertragen im Frequenzband 2,4 GHz (WLAN nutzt mittlerweise auch den 5 GHz-Bereich, Bluetooth 3.0 verwendet WLAN-Verbindungen) und sollen unterschiedliche Geräte über Funk miteinander verbinden. Beide Standards zeichnen sich durch unterschiedliche

– Stärken und
– Geräteunterstützung

aus.

Bluetooth ist mit geringen Hardwarekosten, niedrigem Stromverbrauch und Echtzeitfähigkeit in den Bereichen

– Sprachübertragung,
– Audio/Video-Lösungen und
– Adhoc-Verbindungen zwischen Kleinstgeräten[51]

besser geeignet. Bluetooth löst hier IrDA (Infrarot) erfolgreich ab. Und Bluetooth 3.0 macht sich WLAN-Techniken zunutze, um große Datenmengen zu übertragen[52].

10.12 WiMax

WiMax steht für Worldwide Interoperability for Microwave Access und bezeichnet eine innovative Funktechnologie, die der heute bei Laptops verbreiteten WLAN-Technologie für die drahtlose Datenübertragung ähnelt. Die Reichweite und die Datenübertragungsraten sind jedoch erheblich größer, so dass durch WiMax-Netze ganze Städte mit einem schnellen Internetzugang versorgt werden können. Außerdem zeichnet sich die neue Technologie auch durch Sicherheit und Zuverlässigkeit aus.

Mit WiMax werden nicht nur ganze Standorte wie Wohnhäuser oder Unternehmen mit dem Internet vernetzt, sondern es wird auch möglich, mobile und portable Anwendungen mit Laptop, PDA und Handys zu nutzen.

Der Technologie-Konzern Intel zählt zu den Hauptförderern von WiMax und investiert gemeinsam mit anderen Großunternehmen wie Siemens, Motorola und Samsung in die Entwicklung WiMax-kompatibler Geräte für den Massenmarkt.

---

[51] Bluetooth-(Kleinst-)Geräte sind etwa Mikrofone, Headsets und Handys.

[52] Siehe dazu http://www.golem.de/specials/bluetooth/

WiMax ist drahtlos und unabhängig vom Festnetz. Aus diesen Gründen bietet die neue Technologie gegenüber kabelgebundenen DSL-Anschlüssen bzw. –Zugängen wesentliche Vorteile: Der Internetzugang ist

– flexibler z. B. beim Umzug,
– schneller installierbar durch die moderne Funk-Technologie und
– kostengünstiger dank innovativer Technik.

WiMax ist ein Standard für regionale Funknetze (MAN oder WAN). Allerdings wird WiMax im Moment noch nicht auf breiter Basis eingesetzt und hat daher wenig kommerzielle Bedeutung.

Die WiMax-Technologie wird vor allem in Gebieten eingesetzt, in denen die DSL-Anbindung (über Breitband-/Glasfaserkabel) nicht rentabel oder überhaupt nicht möglich ist. Dadurch, dass die WiMax-Technologie über Funk eine Verbindung zwischen Endnutzer und Breitbandverbindung herstellt, können solche Gebiete von der WiMax-Technologie besonders gut erschlossen werden.

Zunächst einmal sendet WiMax im Gegensatz zu den bisher bekannten Richtfunk-Verbindungen im Mikrowellenbereich zwischen 2 und 66 GHz.

WiMax bietet theoretisch Möglichkeiten, weitaus mehr Kunden zu erreichen und mit einem drahtlosen Internetzugang zu versorgen, als dies im Moment der Fall ist. Dieser wäre zudem schneller und kostengünstiger.

Außerdem würde WiMax endlich eine Möglichkeit für die Telefonanbieter bieten, die so genannte "letzte Meile" zu den Haushalten und damit zu den Endverbrauchern zu überbrücken. Mit der "letzten Meile" ist das Endstück einer Telefonleitung für Datenübertragung gemeint, das für DSL-Anschlüsse entscheidend ist. Weil diese letzte Meile in den Händen der Telekom liegt, werden auch DSL-Anschlüsse zu großen Teilen über die Telekom verwaltet/reguliert.

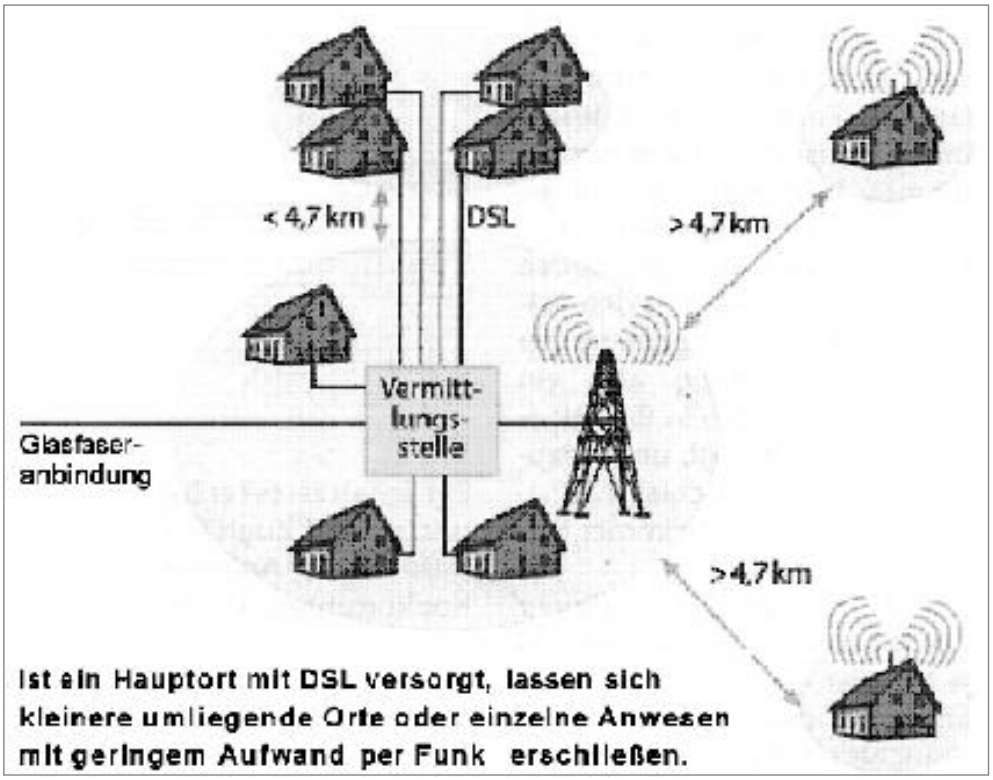


Abb. 32: *Breitband-DSL über WiMax-Verbindung (www.heise.de)*

WiMax würde daher den großen Vorteil bieten, nicht mehr auf diese letzte Meile angewiesen zu sein, wenn man Kontakt zum Endnutzer herstellen will, da WiMax mit Funk arbeitet und große Entfernungen überbrücken kann. Internetdaten könnten also per Funk über die Entfernung zwischen den Endkunden und Hochgeschwindigkeitsnetz übertragen werden.

Zunächst einmal müssen zum Aufbau eines flächendeckenden WiMax-Netzes für mobile Anwender/-innen stationäre Sendeeinheiten bzw. Verteiler eingerichtet werden. Diese Basisstationen müssten in einer Stadt an zahlreichen Orten positioniert werden. Eine solche Basisstation könnte ca. 50 Haushalte gleichzeitig versorgen, je nach Standort der Station.

Grundsätzlich ist geplant, mit dieser Technik sehr hohe Bitraten in einer Größenordnung von 50 MBit/s und mehr, was ein Vielfaches der herkömmlichen DSL-Geschwindigkeit ist, über große Distanzen (mehrere Kilometer) an

– stationäre Internet-Clients (Fixed WiMax) und
– mobile Endgeräte (Mobile WiMax)

zu übertragen.

Hierbei ist mittlerweile erkennbar, dass

– Fixed WiMax und
– Mobile WiMax

eher konkurrierende als komplementäre Technologien sind. Eigentlich wurden sie für unterschiedliche Märkte entwickelt und sollten sich gegenseitig ergänzen – es wird aber kaum vermeidbar sein, dass Mobile WiMax-Lösungen in Marktbereiche von Fixed WiMax einbrechen werden – genau wie breitbandige Mobilfunkangebote den

DSL-Anschluss ablösen werden, wenn eines Tages die Preise für die mobile Datennutzung entsprechend sinken sollten.

Doch wie die Entwicklung tatsächlich verlaufen wird, ist derzeit noch nicht abzusehen. Es gibt Studien, die WiMax hervorragende Zukunftschancen vorhersagen, und andere, die davon ausgehen, dass der Breitband-Funk erst einmal eine Nischentechnologie bleiben wird.

Die typische Reichweite soll zunächst bei etwa 600 Metern liegen, die bei der Versorgung mobiler Endgeräte (z. B. Laptops) in Häusern im städtischen Gebiet mit WiMax erreicht werden kann. Dabei steht dann eine Bitrate von knapp 20 MBit/s zur Verfügung, die sich allerdings alle Nutzer einer Zelle teilen müssen. Vorstädtisch werden bei gleicher Bitrate aufgrund der weniger dichten Bebauung etwa 900 Meter erreicht.

Die WiMax-Technik ist ein drahtloser DSL-Ersatz. Soweit die Antenne der Basisstation ausreichend hoch angebracht ist, lassen aufgrund der geringeren Signalschwächung mehrere Kilometer Reichweite erzielen.

Zudem können mehrere Basisstationen in einer Kette angeordnet werden. Produkte dieser Art sind bereits seit einiger Zeit am Markt verfügbar. Es gibt inzwischen auch erste zertifizierte WiMax-Hardware, die den Vorgaben des WiMax-Forums für Standard-Konformität und Hersteller-Interoperabilität entsprechen. Mit diesen Zertifikationen soll sichergestellt werden, dass WiMax-Geräte verschiedener Hersteller untereinander kompatibel sind.

Es wurden schon Geräte vorgestellt, mit denen die mobile WiMax-Nutzung möglich ist. Insbesondere Intel engagiert sich sehr in diesem Bereich. Mit der Intel WiMax Connection 2300 hat das Unternehmen einen Chipsatz entwickelt, der durch eine einziges Schaltelement sowohl WLAN- als auch WiMax-Übertragung ermöglicht. Weitere Baureihen wurden mittlerweile angekündigt. Intel und auch andere Hersteller wollen diese Chips kurzfristig in ihre neuen Kommunikationsgeräte integrieren.

10.13 Selbstlernaufgaben

1. Begründen Sie, ob sich Bluetooth- und WLAN-Geräte gegenseitig stören können.
2. Erläutern Sie je einen Vorteil und einen Nachteil eines Shared Medium.
3. Wie heißen die Bluetooth Sicherheitsstufen?
4. Worin besteht der grundlegende technische Unterschied zwischen der Datenübertragung über Funkwellen und über Lichtwellen?
5. Welche entscheidenden Nachteile hat die Bluetooth-Technik?
6. Was ist ein Carrier-Sense-Protokoll?
7. Wovon hängt die Reichweite eines Bluetooth-Signals ab?
8. Stellen Sie in einer Tabelle die Unterschiede zwischen einem C/S- und einem Peer-to-Peer-Netzwerk dar.
9. Was ist ein Piconetz, was ist ein Scatternetz?
10. Wofür steht SDP und welche Funktion hat es?

10.14 Zusammenfassung und Ausblick

Mit den aktuellen Funk-Techniken können Sie im LAN- und Heimbereich

– Audio-,
– Video- und
– Kommunikationsgeräte

vernetzen und steuern.

Im Vergleich zu den anderen Funktechniken besticht WiMax durch seine Reichweite und auch durch seine Datenübertragungsgeschwindigkeit. WiMax eignet sich sowohl

– zur Verlängerung des DSL-Glasfaserkabels (WAN/MAN) als auch
– für LAN-Verbindungen.

Welche WiMax-Produkte bald verfügbar sein werden und inwiefern sich diese Technik durchsetzen wird, bleibt abzuwarten.

IrDA (Infrarot-Technik) wird aufgrund

– seiner äußerst geringen Reichweite und
– der notwendigen Sichtverbindung zwischen Sender und Empfänger

weiter an Bedeutung verlieren.

Den Funknetzwerken gehört die Zukunft; die einst kritischen Faktoren

– Sicherheit,
– Geschwindigkeit,
– Umweltverträglichkeit,
– Reichweite

sind in den letzten Jahren stark verbessert worden. Die Kabelnetze sind auf dem Rückzug.

Zwar macht die Entwicklung der Ethernetstandards ebenfalls nicht Halt, doch befinden sich Funk-Technologien auf der Überholspur.

Die Lebenszyklen verkleinern sich, der zeitliche Abstand von Generation zu Generation der Netzwerk-Hardware wird immer kürzer.

Es steigt der Bedarf nach Verbesserungen und auch die Gweschwindigkeit, mit der neue Standards veröffentlicht werden.

Um ein Funknetzwerk auf den neuesten Stand zu bringen, ist oft nur ein Firmwareupdate

– an der Basisstation und
– an den Netzwerkadaptern

notwendig; manchmal müssen zusätzliche Treiber und System-Aktualisierungen eingerichtet werden, zum Teil ist veraltete Hardware auszutauschen und/oder ein aktuelleres Betriebssystem zu installieren.

Beim Ethernet gestaltet sich die Anpassung an neue Standards oft viel problemtischer, da zusätzlich

– Kabel und
– Steckverbindungen

betroffen sind. Gegebenenfalls müssen hier also

– sämtliche Leitungen neu verlegt bzw. ersetzt werden,
– Stecker, Buchsen und Kopplungsgeräte ausgetauscht werden.

Der Aufwand, ein Kabelnetzwerk auf den aktuellen Stand zu bringen, kann daher im Vergleich zum drahtlosen Netzwerk deutlich größer sein.

Im Rahmen dieser Lerneinheit haben Sie das Wichtigste über funkbasierte Netzwerke erfahren. Sie kennen nun die technischen Eigenschaften von WLAN und Bluetooth, die verschiedenen Architekturen und Verbindungsmöglichkeiten im WLAN, wie etwa

– den Infrastruktur-Modus und
– den Adhoc-Modus.

Als wichtigstes Gerät im WLAN-Funknetzwerk haben Sie den Access-Point kennen gelernt. Der Access-Point ist das zentrale Steuerungsgerät eines Infrastruktur-Netzes; er steuert die Datenübertragung zwischen den Knoten bzw. Clients des Netzwerks.

Ein Access-Point übernimmt allerdings auch weitere Funktionen. Je nach lokaler Hardware/Infrastruktur gehört dazu

– die Vernetzung mehrerer WLANs untereinander als Kopplungsgerät im WDS und auch
– die Verbindung eines Ethernet mit einem WLAN.

Die WLAN-Clients kennen

– den festgelegten Netzwerknamen sowie
– die Verschlüsselungscodes;

sie haben somit Zugriff auf die Basisstation.

Im Gegensatz zu WLAN setzen Sie Bluetooth zur Vernetzung von Kleinstgeräten im Nahbereich ein.

Sicherheitslücken von Funktechnologien gehören der Vergangenheit an. Speziell Bluetooth besitzt zuverlässige Verschlüsselungsalgorithmen und Security Levels:

– Non-secure,
– Service-Level,
– Link-Level.

Weitere Informationen zum Thema WLAN finden Sie etwa unter

– http://www.informationsarchiv.net
– http://www.tomshardware.com
– http://www.dslweb.de

– http://www.dsl-magazin.de
– http://wiki.uni-konstanz.de/wlan
– http://www.netgear.de/Support/Basiswissen/wireless_lan_grundlagen.html
– http://wndw.net/

und natürlich auf den Seiten der Hersteller.

Gute Quellen sind auch

– http://de.wikipedia.org/wiki/Wireless_Local_Area_Network bzw.
– http://www.ref.gv.at/Sicherheit___WLAN_Checkliste_-.617.0.html

In der folgenden Lerneinheit geht es um weitere Aspekte in Funknetzwerken; hier werden

– rechtliche Aspekte,
– Sicherheit und
– die Einrichtung eines WLAN

im Vordergrund stehen.

10.15 Hausaufgabe

1. Was ist ein Hop-Key?
2. Gibt es einen offiziellen WiMax-Standard? Wo ist dieser festglegt?
3. Wie erfolgt bei Bluetooth die Verbindung mehrerer Piconetze?
4. Welche Netzwerktopologie findet
   - im Adhoc-Modus,
   - im Bridge-Modus,
   - im Infrastruktur-Modus

   Anwendung?
5. Was ist adaptives Frequenz-Hopping?
6. Welche Funktion hat der Master in einem Bluetooth-Netzwerk?
7. Welche Vorteile hat UWB gegenüber Bluetooth?
8. Was versteht man unter Pairing?
9. Worin unterscheiden sich die Zielsetzungen von WLAN und Bluetooth?
10. Mit welchem Zielkonflikt ist die Erstellung und die kostenlose Verbreitung neuer Firmware verbunden?

10.16 Lösungen zu den Selbstlernaufgaben

1. Zwischen WLAN und Bluetooth sind Störungen möglich, da es gemeinsame Frequenzbereiche gibt.

2. Vorteil des Shared Medium ist, dass parallele Übertragung zu mehreren Rechnern möglich ist, also Übertragungswege gespart werden; Nachteil ist der Geschwindigkeitsverlust, da die Bandbreite geteilt wird.

3. Die Bluetooth-Sicherheitsstufen heißen Non-Secure, Link-Level, Service-Level.

4. Funkwellen breiten sich wellenförmig aus, Kenngröße ist die Frequenz in Hertz. Licht breitet sich geradlinig aus, Kenngröße ist die Wellenlänge in Metern.

5. Nachteile der Bluetooth-Technik sind die sehr geringe Bandbreite (2,1 Mbit/s Downstream) und seine Reichweite (max. 100 Meter), die im Heimbereich allerdings ausreichend ist.

6. Ein Carrier-Sense-Protokoll (Trägererkennungsprotokoll) hört Datenleitungen auf Kollisionen ab und leitet Folgeaktionen ein (etwa Abbruch der Übertragung, um Bandbreite zu sparen).

7. Die Reichweite des Bluetooth-Signals wird durch die Sendeleistung bestimmt:

Geräteklasse	Sendeleistung	Reichweite
1	10,0 mW	100 m
2	2,5 mW	50 m
3	1,0 mW	10 m

8. Client/Server-Netz vs. Peer-to-Peer-Netzwerk

Kriterium	C/S	Peer to Peer
Verwaltung der Ressourcen	Zentral	Dezentral
Lastverteilung	Ja	Keine
Sicherheit	Hoch	Gering
Softwarekosten	Hoch	Gering
Zugriff auf Ressourcen	Einheitlich	Unterschiedlich
Netzwerkgröße	1000e Rechner	Bis 10 Rechner
Administration auf dem Server	Aufwendig, anspruchsvoll	Keine

9. In einem Piconetz sind bis zu 8 Bluetooth-Geräte verbunden. Ein Scatternetz ist ein Verbund mehrerer Piconetze.

10. Das Service Discovery-Protokoll SDP dient der Erkennung Bluetooth-fähiger Geräte im Netzwerk.